# Part I

# Applying intelligence

# 1 Traditional intelligence practice

## Introduction

This chapter traces the origins and functions of intelligence practice in the 'traditional' environments of national security and policing. It has two aims: first, it will provide a brief overview of how intelligence historically has been applied in Australia, Canada, New Zealand, the UK and the USA. This overview provides a broad thematic discussion of major historical milestones, which have been important in shaping the development of traditional intelligence practice. This discussion sets the scene for further in-depth development of themes, concepts and issues raised in the three Parts of the book (Applying intelligence, Understanding structures and Developing a discipline). Second, the chapter will argue, based on the origins of traditional intelligence practice, that a set of common characteristics has developed, which help to delineate the uniqueness of 'intelligence' from related activities such as research, analysis and information management. I have called these three characteristics an evolving *intelligence tradition.*

While others may argue for a different set of characteristics – even a long list – it is clear from the historical review in this chapter that these characteristics represent at the very least how intelligence has been viewed in the past. This intelligence tradition will continue to shape how traditional approaches to intelligence are applied, but is also relevant to defining understanding how new intelligence structures, processes and methods are being used in emerging areas of intelligence practice discussed in Chapter 2.

## The origins and functions of traditional intelligence practice

### *National security intelligence practice*

Defining 'intelligence' in a generic sense, let alone national security intelligence, is contentious, different perspectives are included or excluded depending on the view of the scholar or practitioner. I will not engage in these debates here, and national security intelligence is defined as intelligence collected, analysed and disseminated for decision-makers in the support of the security of the state.

By 'security of the state', I mean not just the prevention or prosecution of wars *between* states, but also security of individuals *within and between* states. The definition draws on the human security agenda, which gained momentum in the mid-1990s (Hampson *et al*. 2002). The *Human Security Report* (HSC 2005) includes the security of people within states from political violence (terrorism, civil war, state collapse), economic vulnerabilities and even disease and natural disasters. This inclusive definition of security is more accurate in tracing how national security intelligence has evolved and responded since the end of the Second World War from a preoccupation with fighting or preventing wars between states to currently supporting a broader human security agenda.

In addition to defining national security intelligence, it is also equally difficult to plot its origins. Intelligence historian David Kahn suggests that the Ancient Egyptians used 'codes' on the walls of their monuments (1996: 71–73), and most students of intelligence will be familiar with the work of fourth-century BC Chinese general Sun Tzu, *The Art of War.* Sun Tzu used a network of spies to gain information about the military capabilities and intentions of enemies (Sun Tzu 2002). The focus here is the broad developments within national security intelligence from the end of the Second World War up to the present, as it was not until this period that we saw the emergence of national civilian intelligence operations with global reach.

Table 1.1 provides a summary of the origins and functions of the major national security intelligence communities of Australia, Canada, New Zealand, the UK and the USA. Broadly, the functions of many agencies across each country are similar. For example, in Table 1.1 it is clear that the UK MI6 and the Central Intelligence Agency (CIA) are involved in the collection of foreign intelligence, and each country has a dedicated sigint collection agency (sigint is a general term for the process of collecting intelligence from intercepted electromagnetic waves, usually referred to as signals). There are of course, several differences between and even within the national security intelligence communities of the countries listed in Table 1.1. Historically, variations have emerged as a result of different organizational structures, political cultures, legal systems and bureaucratic styles, existing in each of these countries.

The historical significance of many of these factors has been well documented, particularly relating to the US and UK communities, in a growing number of volumes on the history of various intelligence agencies. Christopher Andrew's book, *The Defence of the Realm: The Authorised History of MI5* (2009) is a good recent example. However, despite each intelligence agency in Australia, Canada, New Zealand, the UK and the USA following its own historical path, their origins and functions were also shaped by some similar events from the end of the Second World War, through the Cold War and up to the present. The events from 1945 to the present day did help define mutual interests and common values between the intelligence communities of these countries. Mutual interests and broadly similar liberal democratic outlooks also resulted in commonalities developing both within and between intelligence agencies in structure, priority setting and accountability processes.

A detailed discussion of all historical events that have impacted the origins and functions of all national security agencies in each country is beyond the scope of this book. In the USA alone, there are 17 agencies officially designated as part of its national security intelligence community and an entire book could easily be devoted to them alone. Instead, subsequent chapters will examine a selection of thematic changes (e.g. organizational restructure, analytical innovations and legislative reform) in the national security intelligence agencies of the five democratic countries chosen as the subject of this study and how these help us understand the evolution of national security and other practice contexts for intelligence. However, in order to provide some context for this discussion, it is important first to understand the broad historical catalysts for change in national security intelligence agencies from the end of the Second World War to the present.

### *From post Second World War to post Cold War*

Wartime intelligence cooperation between the five allies (Australia, Canada, New Zealand, the UK and the USA), particularly between America and the UK, set the stage for common approaches and cooperation during the Cold War period. Wartime technological advancements such as signals intelligence (sigint), overhead imagery and counter-intelligence also produced greater modernization, specialization and cooperation between the national security intelligence communities in the five countries. These intelligence arrangements became even more formalized in the Cold War period, starting with the 1946 UK/USA Communications Intelligence Agreement, where the five countries agreed to share their sigint collection efforts with each other. This agreement stipulated that the following sigint agencies would share their intelligence: the National Security Agency (the USA), Government Communications Headquarters (the UK), Communications Security Establishment (Canada), the Government Communications Security Bureau (New Zealand) and the Defence Signals Directorate (Australia).

The UK/USA Communications Intelligence Agreement led to some geographical specialization between each country's sigint collection agency. The agreement has been tested through the years, most notably in 1985, when the USA restricted its sigint supply to New Zealand after that country banned nuclear-powered vessels from its ports. The agreement also provided the basis for closer cooperation in other areas of intelligence practice, including humint (human intelligence) and sharing intelligence products. The desire by the USA in particular, but also the other four UK/USA Agreement countries, to contain Soviet interests globally became the central focus for all of their national security intelligence agencies. At the conclusion of the Second World War and the early stages of the Cold War, other non-state actor security interests were largely subservient to or viewed through the prism of the broader Soviet threat. The dominant application of national security intelligence efforts in the latter half of the twentieth century up to the end of the Cold War in 1991, focused on expensive technical intelligence gained from satellite reconnaissance and sigint. The height of the Cold War was more than anything a 'sigint war' between the USA and the Soviet Union. The successful

*Table 1.1* Origins and functions of select national security agencies

| *Types of intelligence* | *The UK* | *The USA* | *Australia* | *Canada* | *New Zealand* |
|---|---|---|---|---|---|
| Signals Intelligence | Government Communications Headquarters (GCHQ)<br>*Est.: 1919* | National Security Agency (NSA)<br>*Est.: 1952* | Defence Signals Directorate (DSD)<br>*Est.: 1947* | Communications Security Establishment Canada (CSE)<br>*Est.: 1946* | Government Communications Security Bureau (GCSB)<br>*Est.: 1977* |
| Foreign Intelligence (humint*) | Secret Intelligence Service (MI6)<br>*Est.: 1909* | Central Intelligence Agency (CIA)<br>*Est.: 1947* | Australian Secret Intelligence Service (ASIS)<br>*Est.: 1952* | No specific foreign intelligence agency, but CSE provides some foreign intelligence collection via its sigint capabilities. | New Zealand Security Intelligence Service (NZSIS)<br>*Est.: 1956* |
| Domestic Intelligence | Security Service (MI5)<br>*Est.: 1909* | 1. Federal Bureau of Investigation (FBI)<br>*Est.: 1908*<br>2. Department of Homeland Security (DHS) – *Offic of Intelligence and Analysis*<br>*Est.: 2003* | Australian Security Intelligence Organisation (ASIO)<br>*Est.: 1949* | Canadian Security Intelligence Service (CSIS)<br>*Est.: 1984* | NZSIS |
| Intelligence Assessment | 1. Joint Intelligence Committee (JIC)<br>2. Joint Terrorism Analysis Centre (JTAC)<br>*Est.: 2003* | 1. Office of the Director of National Intelligence (ODNI)<br>*Est.: 2005*<br>2. CIA<br>*Est.: 1947*<br>3. Bureau of Intelligence and Research (INR)<br>*Est.: 1946*<br>4. National Counterterrorism | 1. Office of National Assessments (ONA)<br>*Est.: 1977*<br>2. National Threat Assessment Centre (NTAC)<br>*Est.: 2004* | 1. Intelligence Assessment Secretariat (IAS)<br>2. Integrated Threat Assessment Centre (ITAC)<br>*Est.: 2004* | 1. National Assessments Bureau (NAB)<br>*Renamed March 2010 (formerly the External Assessments Bureau)*<br>2. Combined Threat Assessment Group (CTAG)<br>*Est.: 2004* |

| | | | | | |
|---|---|---|---|---|---|
| | | Center (NCTC)<br>*Est.: 2004* | | | |
| Military Intelligence | 1. Defence Intelligence Staff (DIS)<br>*Est.: 1964* | Defense Intelligence Agency (DIA)<br>*Est.: 1961* | Defence Intelligence Organisation (DIO)<br>*Est.: 1990* | Department of National Defence/Canadian Forces – Director of General Intelligence Production | Directorate of Defence Intelligence and Security<br>*Est.: 1998* |
| Imagery Intelligence | Defence Geographic and Imagery Intelligence (DGIA)<br>*Est.: 2000* | 1. National Reconnaissance Office (NRO)<br>*Est.: 1960*<br>2. National Geospatial Intelligence Agency (NGA)<br>*Est.: 2003 (prior to 2003 formerly the National Imagery and Mapping Agency (NIMA))* | Defence Imagery and Geospatial Organisation (DIGO)<br>*Est.: 2000* | Directorate of Geospatial Intelligence (D Geo Int) | NZDF Geospatial Intelligence Organisation<br>*Est.: 2008*<br>*(prior to 2008 formerly the Joint Geospatial Support Facility)* |
| Agencies with national policing/law enforcement functions | Metropolitan Police<br>*Est.: 1829* | FBI<br>DHS | Australian Federal Police (AFP)<br>*Est.: 1979* | Royal Canadian Mounted Police (RCMP)<br>*Est.: 1920 (formerly the North-West Mounted Police (Est.: 1873))* | NZ Police<br>*Est.: 1886* |
| Organized Crime | Serious Organised Crime Agency (SOCA)<br>*Est.: 2006* | FBI | Australian Crime Commission (ACC)<br>*Est.: 2003* | Criminal Intelligence Service Canada (CISC)<br>*Est.: 1970* | Organised Financial Crime Agency of New Zealand (OFCANZ)<br>*Est.: 2008* |

* Intelligence collected by humans either through covert means (e.g. espionage) or through official channels (e.g. diplomatic liaison).

prosecution of this war relied on sigint collection agencies having strict control over the knowledge relating to their collection capabilities and which aspects of Soviet capabilities they were targeting. The absolute secrecy adopted by sigint collection agencies contributed significantly to a developing culture of secrecy within national security intelligence agencies during the Cold War and up to the present.

While significant sums were invested in UK/USA Agreement countries' intelligence agencies, these agencies were not able to predict the collapse of the Soviet Union, the country which had been their key threat from 1945 to 1991. The mixed track record of many agencies during the Cold War, and the emergence of a fluid security environment – no longer defined by US–Soviet rivalry – raised questions from some academics, commentators and politicians about the future relevance of such agencies (e.g. Gill 1996a; Draper 1997). Additionally, the incoming first Bush Administration – using the rhetoric of a 'peace dividend' derived from defeating the Soviet Union – was focused on maximizing any savings that could be made from defence and intelligence budgetary allocations. In the 1990s, the Bush and Clinton Administrations, along with Congress, decreased intelligence budgets. For example, during the 1990s, the CIA's budget declined by 18 per cent, which resulted in a 16 per cent reduction in its workforce during this decade (Tenet 2002). Similarly, in 1996, the UK Treasury initiated cuts, which led to a reduction in MI6 staffing levels to about 2150 (Dorril 2001: 780). The collapse of the bipolar security structure of the USA and the Soviet Union revealed a greater diversity of threats, such as international terrorism and drug trafficking, which national security intelligence agencies had always monitored, however, during the height of the Cold War they were not seen as existential threats to the state.

Hence, the first half of the 1990s could be typified as a time of adaptation by national security intelligence agencies to an evolving and less certain security environment. Agency heads were starting to show an increased awareness of, if not complete understanding of, myriad transnational security threats, which progressively began to define the new security environment. On 2 February 1993, R. James Woolsey commented to the Senate Select Committee on Intelligence (SSCI), just before he was confirmed as Director, Central Intelligence, that the security environment was changing. Woolsey, who served as Director of the CIA from 1993 to 1995, described both the complexity of the new security environment and the need for intelligence in the following colorful way: 'We have slain a large dragon by defeating the Soviet Union, but we live now in a jungle filled with a bewildering variety of poisonous snakes, and in many ways the dragon was easier to keep track of' (Woolsey, quoted on Center for Intelligence Studies website). The statement reflected the difficulty that agencies such as the CIA were having in adjusting their collected and analytical assets from a single large and enduring target (the Soviet Union) to a multitudinous number of smaller and more fluid targets. For national security intelligence agencies, efforts to recalibrate intelligence collection assets were made more difficult as policy-makers failed to provide them consistently with a clearly articulated list of their priorities. For example, under the first Clinton Administration, despite some efforts to remedy the collection

and analytical priorities framework, terrorism remained a 'Tier 3' (lowest priority issue) (FAS 1995). Despite several Islamist terrorist plots and attacks against US interests from 1993 up to 9/11, including Al Qaeda's October 2000 assault on the US warship *USS Cole* in Yemen, the Bush Administration still had rogue states and their weapons of mass destruction (WMD) as its highest priority (Taylor and Goldman 2004: 425). However, there is no doubt by the end of the 1990s, Australian, Canadian, New Zealand, UK and US intelligence agencies had all developed a sophisticated understanding of the transnational national terrorist threats, particularly of the Al Qaeda 'brand'.

## 9/11, accountability and the commodification of intelligence

However, the events of 9/11, the first mass casualty terrorist attack on US soil, represented a 'wake-up call' for the US intelligence community. They also had strategic significance for the intelligence communities of Australia, Canada, New Zealand and the UK. Additional events after 9/11 including the nature of intelligence supplied to political leaders about the presence of WMD in Iraq in 2003, the Bali bombings (in October 2002) and the London bombings (in July 2005), also resulted in significant internal reflection for the US, UK and Australian intelligence agencies on their collection and analytical capabilities against such threats. For Canada, the 'wake-up' call for their national security intelligence agencies was not 9/11, but an event nearly two years earlier on the US-Canadian border. When interviewed on 26 August 2009, two senior Canadian Security Intelligence Service (CSIS) officers suggested that the foiled December 1999 attempt by Canadian-Algerian Ahmed Ressam to blow up Los Angeles International Airport became the major catalyst for a greater shift in focus by their agency from counter-intelligence to counter-terrorism. The underlying concern for CSIS officers was that Canada could be a base for attacks against its major trading partner, the USA.

The two significant inquiries after 9/11 – the House and Senate Intelligence Committee's Joint Inquiry (2002) and the 9/11 Commission Report (2004) – produced a series of findings about deficiencies within the US intelligence community, particularly the CIA and the Federal Bureau of Investigation (FBI). Reported deficiencies were numerous, ranging from human error, problems with analysis, collection and information sharing. In many respects, the deficiencies identified reflected earlier issues already noted in at least 14 major studies on intelligence reform from 1995 to 2002 (Zegart 2007: 199–200). The outcomes of the post-9/11 era inquiries have been a great deal of introspection by academics and practitioners about how fit for purpose and accountable national security intelligence agencies are (e.g. Hitz and Weiss 2004; Zegart 2007). The discourse of 'intelligence failure' has become popular again long after Richard Betts' seminal study of the subject in 1978 (Betts 1978). Chapter 6 will explore 'intelligence failure' and 'intelligence reform' more closely and how managers can use the 'lessons learnt' from recent inquiries to promote better practice and organizational adaptability. However, the post-9/11 inquiries in the USA, the UK and Australia were different from earlier ones in two major respects.

First, as discussed further in Chapter 4, key recommendations from these inquiries have resulted, in many cases, in major structural changes to intelligence communities not seen for decades. In particular, changes in the USA include the creation of the Department of Homeland Security (DHS) and the Office of the Director for National Intelligence (ODNI). Second, the post-9/11 inquiries have become much more public and politicized processes than their predecessors. The public, politicians and the media engaged actively in the flurry of post-9/11 inquiries, frequently expressing their frustration over what they perceive as a series of 'intelligence failures', including 9/11, Iraq, the London bombings and the Bali bombings. Governments have become aware of a lack of public confidence in some national security intelligence agencies and as part of their review and reform processes have pushed these agencies to provide more public insight into their roles and the accountability mechanisms governing them, where possible. Recommendation 23 of the Flood Report (a study of Australia's intelligence community), illustrated the point by suggesting that an unclassified brochure should be published describing the role of each agency (Flood 2004: 185). The other factor influencing the extent to which national security intelligence has become a 'public commodity' has been the more proactive approach being taken by these agencies towards counter-terrorism since 9/11. New counter-terrorism laws and enhanced investigative powers, hastily drafted after 9/11, have meant, in the words of one former CIA officer Charles Cogan, that agencies are not just passive recipients of intelligence but active 'hunters' as well (quoted in Gill and Phythian 2006: 76). As discussed in Chapter 10, the urgency in attempting to prevent the next terrorist attack and a more aggressive approach to intelligence collection and operational activity have resulted in a number of ethical and legal dilemmas for national security intelligence agencies, which has ensured they stay in the public spotlight. This is unlikely to change in the near future as national security intelligence agencies seek to balance secrecy, including their use of proactive intelligence collection, and targeting with greater legislative, political, judicial and public scrutiny.

In summary, the origins and functions of the UK and US national security intelligence agencies have developed partly organically and by design. Their development has been driven by the changing nature of the security environment in particular (from focusing on the Soviet Empire to chasing global outlaws such as transnational terrorists), and their ability to adapt to it. Change has also been driven internally by management via a diverse array of bureaucratic initiatives (see Chapter 6) and externally through political, legal and parliamentary oversight mechanisms (see Chapter 7). Increasingly, the contemporary security environment has also resulted in the blurring of boundaries between national security and other intelligence disciplines (policing and private sector). Attempting to 'join the dots' of myriad new threats in this complex environment questions the validity of historical and Cold War parameters of what national security, foreign, military or domestic intelligence are.

While greater cooperation between national security agencies under the UK/USA Agreement has facilitated even closer working relations in the post-Cold War period, even now in the post-9/11 world of 'need to share' information, many of

these agencies remain bound by their own traditions. The cultures of secrecy forged during the Cold War have not disappeared and this means that not all intelligence can be shared automatically or promptly even with friends outside the UK/USA Agreement, such as in NATO (Clough 2004: 608). Other customs, norms, technological practices, which have long been the hallmark of many of their secret surveillance and covert operations, remain.

For the foreseeable future it's unlikely that the first two aspects of what I refer to as the evolving intelligence tradition – *the culture of secrecy* and detailed knowledge of *secret surveillance techniques* – will be challenged completely by governments or commentators. However, since 9/11, national security agencies have become increasingly public and political commodities and in that sense some of the 'mystery gloss' has been rubbed off. In many respects, now they are becoming just like other bureaucratic agencies, where the public and their political masters are increasingly interested in seeing if their operations are ethical, legal and value for money.

## Policing intelligence

In contrast to the small number of agencies which comprise the national security intelligence communities of the UK/USA Agreement countries, the number of policing agencies in each country, with the exception of New Zealand, is generally larger. New Zealand has only one policing agency, while the UK, the USA, Canada and Australia have several agencies with differences in jurisdictional responsibilities. For example, the USA has approximately 18,000 and Canada has 380 policing agencies. Examining the origins and functions of all their intelligence capabilities is therefore not possible in this volume. Instead, the focus will be on the key thematic and historical factors which have shaped the development and origins of policing intelligence in Australasia (Australia and New Zealand for brevity will be discussed in the same section), Canada, the UK and the USA. Given the limited space, discussion will also centre on specific agencies due to the relative impact they have had in their country on policing intelligence developments, and to highlighting specific themes for closer study in subsequent chapters. For example, it is difficult not to talk about the origins and functions of US policing intelligence without examining the FBI, or similarly developments in the UK without looking at the Metropolitan Police. There are also other agencies which could be discussed here including those which have some policing powers or others with more enforcement or regulatory functions (for example, revenue, immigration, customs), but discussion here is restricted to traditional policing agencies.

### *UK developments*

Grieve provides a comprehensive summary of historical developments in UK policing intelligence. He suggests that 'Intelligence as a discipline had been known to UK public policing, as early as 1805, and with the Metropolitan Police its earliest connections were also with military intelligence.' The link with military

intelligence resulted in the early use by the police of informants and surveillance to support investigations (Grieve 2009: 30–46). Historically, UK policing intelligence derived from a combination of external and internal factors. Leadership and the managerial reform initiatives of chief constables and commissioners have obviously been an important internal factor. The increased uptake in technology from the 1960s onwards has also transformed all aspects of policing, including intelligence. Technology has allowed greater specialization within policing intelligence in areas such as crime analysis – a topic discussed in greater detail in Chapter 8.

The external factors arguably are more important in understanding the development of UK policing intelligence, and the role of a series of oversight measures and institutions has been particularly relevant in shaping intelligence capabilities. Since the 1970s, government and formal professional oversight initiatives have culminated in the creation of a more formalized, structured and legislated approach to policing intelligence in the UK compared to most other agencies in Australia, Canada, New Zealand and the USA.

Collectively, a number of oversight bodies, including the role of the UK Home Office, Her Majesty's Inspectorate of Constabulary (HMIC) and the Associations of Chief Policing Officers (ACPO), and the National Policing Improvement Agency (NPIA) have achieved a lot more influence on the development of UK policing intelligence capabilities than their counterparts in other countries discussed in this section. The HMIC is an independent advisor on UK police services and carries out regular inspections relating to their overall efficiency and effectiveness. In recent years it has completed a series of thematic inspections relevant to intelligence practice (HMIC 1997, 2000, 2005). The HMIC 1997 report, *Policing with Intelligence*, was particularly important in promoting proactive intelligence approaches into UK policing. ACPO is an independent professional body made up of the senior executives of the police services of England, Wales and Northern Ireland. It works with other stakeholders such as the HMIC, the Home Office and the Association of Police Authorities to promote leadership and the development of better doctrine across various policing areas. ACPO has also been active in the promotion of better policing intelligence in the UK through a series of reports known as the Baumber Report (ACPO 1975), the Pearce Report (ACPO 1978) and the Ratcliffe Report (ACPO 1986). The Baumber Report was influential in shaping modern UK policing intelligence in recommending standardized approaches for setting up force intelligence units across each of the 43 (English and Welsh) forces. The Pearce and Ratcliffe Reports looked at the establishment of regional criminal intelligence offices and field intelligence officers respectively. We will come back to a more detailed discussion of these reports in Chapter 6 in the context of how they are useful in helping managers and leaders focus on creating appropriate organization structures for policing intelligence today. The NPIA has a reforming role and works with the ACPO, the Home Office and individual forces to develop skills, professionalism, doctrine and capabilities in various policing areas. It has been very active in providing resources and training for policing agencies to enhance their compliance to the National Intelligence Model (NIM) – developed

in 2000 to promote a common approach to intelligence across all English and Welsh forces.

Another important external driver impacting on the development of UK policing intelligence was the emergence in the 1990s of a 'New Public Management' ethos that was focused on maximizing cost efficiencies and effectiveness across the public sector. At this time there was growing political pressure for police to demonstrate the use of their limited resources more effectively. The 1993 Audit Commission report *Helping with Enquiries: Tackling Crime Effectively*underlined growing concerns within the government that police agencies needed to make better and more proactive use of their resources. This report, together with *Policing with Intelligence* (HMIC 1997), was critical to the evolution of intelligence-led policing approaches within UK policing. I will not dwell on the intelligence-led policing approach here as it will be discussed in more detail in the context of discussion of the NIM in Chapter 4. Ratcliffe (2008) also provides a comprehensive discussion of the development of intelligence-led policing in the UK for those wishing further detail. Suffice it to say, it is an approach that has generated discussion, particularly on agreeing on a single acceptable definition. Ratcliffe's discussion of intelligence-led policing suggests that the emphasis is on using intelligence proactively to target the main or serious offenders or crime problem areas in order to detect, or disrupt their activity (ibid.: 72–73).

Finally, the changing security environment has also been important in influencing the development of UK policing intelligence capabilities. Greater specialization within UK policing intelligence came early with the evolving security threat posed by Irish Republican terrorism. For example, the Metropolitan Police had developed a Special Branch in 1883 to deal with it and increasingly from the 1960s onwards all forces had developed their own special branches (Gill and Phythian 2006: 43). Early on these branches coordinated their activities with MI5 priorities and acquired intelligence using similar surveillance techniques to those used by national security agencies. This close relationship between police and security services fostered better working relations and mutual understanding of each other's work which was important when 9/11 and the 7/7 2005 bombings on London's transport networks occurred. The increasingly complex security environment of global terrorist networks, drug trafficking and people smuggling has also resulted in the emergence of new organizations and bureaucratic arrangements such as the Serious Organised Crime Agency (SOCA) in 2005 and the Joint Terrorism Analysis Centre (JTAC) in 2003. We will discuss these initiatives more fully in Chapter 4.

However, more importantly, the increasingly complex security environment and a growing reliance in UK policing on intelligence-led policing approaches have also resulted in a greater emphasis on proactive applications of intelligence aimed first to *disrupt* threats then build a case for prosecution (Innes and Sheptycki 2004). This is a break with the past, where the emphasis was reacting to a crime, and using intelligence retrospectively to build a chain of evidence for prosecution. Since 9/11, the shift in UK policing emphasis from prosecution to disruption is due to a combination of factors, including government pressure, limited resources and new legal frameworks that allow more proactive and interventionist approaches to

intelligence collection. However, as we shall see in Chapter 7, the move towards proactive intelligence collection and operations has not been without their ethical, legal and social ramifications in the UK and elsewhere. In the UK over the past decade, various mechanisms have been introduced to control how policing intelligence is practised, such as the Regulation of Investigative Power Act 2000 (UK) and the introduction of a Surveillance Commissioner. Yet despite these, ethical, legal, social and operational implications are emerging with the shift towards more proactive and disruptive intelligence operations, particularly in the organized crime and counter-terrorism context (Innes and Sheptycki 2004: 22). The Independent Police Complaints Commission (IPCC) inquiry (the Stockwell Inquiry) into the shooting of the Brazilian Jean Charles de Menezes in July 2005 also underscored some of the adverse implications of a more proactive intelligence approach in a fast moving counter-terrorism operation (IPCC 2007).

Several challenges remain for UK policing intelligence and these are shared to a greater or lesser degree by policing agencies elsewhere. These challenges will be explored thematically in subsequent chapters, but include among others: cultural attitudes within some agencies about the role of intelligence in strategic and operational decision-making, better coordination and integration of intelligence databases with police information management systems, stronger strategic intelligence capabilities and assessing how the NIM may need to be adapted to future policing requirements.

### *Canadian developments*

Most of Canada's older police forces appeared in the 1830s and 1840s, and in contrast to the UK, the origins of Canadian policing intelligence was shaped by the need early on to deal with huge distances between provinces and even some towns. Given there are 380 Canadian policing agencies, a thematic discussion of the origins and functions of Canadian policing intelligence is provided. Instead, I will restrict discussion here to the Royal Canadian Mounted Police (RCMP), which emerged from an earlier incarnation called the North-West Mounted Police, established in 1873. While the RCMP is not representative of all Canadian agencies, its national reach and close involvement with all policing intelligence developments in Canada provide insight into general policing intelligence trends in Canada. Particular trends relevant to the development of policing intelligence in Canada include changes to intelligence models, management, legislation and education issues.

Early specialization in Canadian policing was the catalyst for the gradual development of an intelligence capability in Canadian agencies. For example, as early as 1900, detective squads began to emerge and their further specialization in the 1950s and 1960s (e.g. vice and homicide squads) were important early markers in the development of policing intelligence in Canada (Hamilton 2006: 63). Another important developmental milestone in the 1960s in Canada was the country's early response to a growing organized crime problem, which was emerging in some of its large multi-ethnic cities such as Toronto and Vancouver. The creation

of the Criminal Intelligence Service of Canada (CISC) in 1970 with a central bureau in Ottawa and nine provincial ones was an early attempt to provide a clearing house for sharing intelligence and analysis of organized crime across Canadian policing agencies (CISC 2009).

An early win for CISC was its creation in 1976 of the Automated Criminal Intelligence Information System (ACIIS), which allowed the gathering and sharing of intelligence across Canada's criminal intelligence community. A new criminal intelligence sharing platform is currently being conceived to replace the ACIIS platform (see Chapter 4). CISC is used by over 380 agencies at federal, provincial and municipal levels of policing. It has played an important role in the policing intelligence architecture of Canadian policing, particularly in developing a national threat picture and strategic intelligence analysis. From the early 1960s and up to the 1990s, other policing and analytical models such as community policing and crime mapping were also influential in the developing intelligence capability in Canadian agencies. In particular, the early application of community policing in dealing with organized crime across Canada was useful for building up intelligence collection and analysis.

Hamilton suggests that the growing diversity of Canada's criminal environment, particularly from the early 1960s to the present, made community policing strategies appealing for policing intelligence. He notes:

> Besides the traditional mafia, outlaw bike gangs and the Franco-Montreal underworld, new exceptionally violent players had appeared on the scene: new Chinese Triads, the Russian Mafiya, Haitians in Montreal, the Jamaican Posses in Ontario, violent Sikhs in the aftermath of the Babbar Khalsa insurgency, and the newly arriving Tamil Tiger supporters from Sri Lanka gave Canada a lot of experience in community policing initiatives.
>
> (Hamilton 2006: 70)

Community policing initiatives were also used by the RCMP in a 1985 terrorist investigation, where most of the suspects were from the Punjabi community in British Columbia (Deukmedjian and de Lint 2007). A second major theme in the historical development of Canadian policing intelligence is *accountability*. The 1981 McDonald Commission is arguably the most important example of how accountability has played an important role in shaping the origins and functions of Canadian policing intelligence. A full summary of the Commission's findings can be found in the study by the McDonald Commission (McDonald 1981b: 513–514). But the key recommendation of the Commission was for a new legal and organizational structure for Canadian national security intelligence, which would remove this responsibility from the RCMP and give it to a new civilian security intelligence agency, the CSIS in 1984. Until 1984, the RCMP's Security Service had been responsible for investigating threats to national security. With this responsibility now shifting to CSIS, the CSIS Act 1984, which created the new agency, was also important to policing intelligence in defining how CSIS would enter into joint activities with Canadian police forces. Cooperation and

coordination, however, between the intelligence activities of CSIS and the RCMP were not optimal in the early years following the creation of CSIS.

This lack of cooperation became apparent following an official review of Canadian security and policing responses to an Air India bombing incident in 1985, when British Columbia-based Sikh radicals put two bombs on flights connecting to other Air India flights. The review by the Security Intelligence Review Committee (O'Connor 2006: 48) did highlight some patch protecting and suboptimal coordination of investigative efforts between it and the RCMP. However, increasingly in the 1990s, as the threats posed by transnational crime and terrorism grew, CSIS and policing agencies, particularly the RCMP, gradually became used to working with each other more effectively, and efforts have been made to forge greater understanding between the two agencies' operational methodologies. In 2009, one senior CSIS officer advised that a joint management team between the two agencies has been established to better coordinate their intelligence-led operational activity. There have also been more recent political and judicial reviews since the 1980s, such as the Arrar Commission, which have also focused on aspects of policing intelligence practice in Canada. The significance of some of these more recent reviews and their legislative impacts on policing intelligence in Canada will be discussed further in Chapter 7.

In summary, the origins and functions of Canadian policing intelligence have been driven broadly by similar themes found in other countries. Greater specialization in policing and intelligence methodologies has been important as have the early development of national coordinated responses to policing intelligence, with the creation of CISC. However, there have also been events unique to Canada that explain the development of policing intelligence there. The creation of a new national security intelligence agency out of a national policing agency is one interesting example. This common heritage between Canada's policing and security intelligence agencies has fostered the cross-fertilization of methodologies with CSIS and RCMP officers moving back and forth between the two agencies. In addition to promoting common understanding, it also helped foster the development and innovation of other more recent intelligence models such as intelligence-led policing (Hamilton 2006: 51).

Finally, another important factor driving review and reform in Canadian policing intelligence has been the willingness, at least periodically, by policing executives to experiment with new ideas or sponsor change. For example, Deukmedjian (2006) argues that it was the failure of community policing strategies that was a key driver for the RCMP adopting an intelligence-led policing response instead in December 2000. Chapter 4 provides a detailed discussion of current innovations in Canadian policing intelligence, including recent work being done within the RCMP and the CISC to develop a Canadian Criminal Intelligence Model (CCIM).

***US policing intelligence developments***

As discussed earlier, the large number of federal, state and local policing agencies in the USA, approximately 18,000, has resulted historically in a fragmented response to policing and policing intelligence (Ratcliffe 2008: 24). There are many historical reasons for this fragmentation. The political culture of the USA is one factor, where there has been a natural suspicion since independence of power being concentrated in one or two authorities. The gradual but unplanned settlement of large parts of the USA, particularly its central and western areas as late as the nineteenth century, also contributed to the fragmented state of US policing today. Whatever the causes for this fragmented response to policing, it remains the single most important feature in not only understanding the historical origins of US policing, but also what has been possible and what is not possible in its practice. See Carter for a brief overview of US policing intelligence (Carter 2004: 21–36). The main point that emerges from even a cursory review of US policing history is that it is not possible to talk about policing intelligence in any discernible sense until the mid to late nineteenth century. As Jeffreys-Jones notes:

> The institutions of the relatively new republic were still being organized, across the country – indeed the US Congress only established the Department of Justice in July 1870. And the establishment of the FBI was not to be for another 38 years.
>
> (2007: 3)

A major historical factor in understanding US policing from its earliest period to the present is the role the US political culture has played in its development. In addition to suspicions over the concentration of power, race politics, anti-communism, an innate public suspicion of surveillance, and bureaucratic rivalries between security and policing agencies, have all played a role in how policing intelligence evolved in the USA. The Bolshevik Revolution in Russia was to play a significant role in shaping the political culture of the USA for generations, including the national level policing intelligence culture. J. Edgar Hoover, Director of the FBI from 1924 until his death in 1972, raised concerns by many in the community about the extensive misuse of his agency's intelligence capabilities against innocent US citizens, particularly during the McCarthy period. Historian Jeffreys-Jones summarizes this period well, arguing that the FBI was the creation of progressives in the 1870s, however, during the McCarthy period it was becoming repellent to liberals (ibid.: 11).

The net result of such abuses at federal and state policing agencies resulted in the closing down of many police departments, which had an impact on their ability later to develop effective criminal intelligence capabilities (Carter 2004: 26). The other noteworthy event, which shaped US political culture and the trajectory of US national policing intelligence, was the passing of the National Security Act of 1947. The National Security Act created the CIA. The CIA was meant to provide a centralized approach to intelligence and the director of the new agency would

also be given control over all aspects of intelligence (military, sigint and the FBI). The Act was seen by Hoover as a wing-clipping for the FBI as his agency – now more formally constraining the Bureau to domestic intelligence gathering rather than abroad. Hoover held the CIA in little regard and this led frequently to intelligence hoarding or lack of cooperation between the two agencies. Relationships between the CIA and the FBI ebbed and flowed under different leaderships post-Hoover and this remained a problem up to 9/11 (Hulnick 2004). Leaving the organizational cultural issues between the CIA and the FBI aside, the unifying and coordinated objectives sought by the National Security Act for US intelligence arguably resulted in the opposite – a more fragmented approach to domestic and international security issues.

More recently, attempts have been made to address this fragmentation of policing intelligence with initiatives such as the Regional Information Sharing Systems (RISS) network, which is used as a formal method of passing criminal intelligence between agencies. In the post-9/11 environment, several initiatives have been implemented; partly to overcome the lack of coordination between the intelligence functions of US policing intelligence agencies, but also to promote better practice underpinned by intelligence-led policing approaches. One example is the National Criminal Intelligence Sharing Plan sponsored by US Chiefs of Police, aimed at promoting greater coordination and common practice approaches (GIWG 2003).

The post-9/11 intelligence field has also seen the growth of fusion centers where several agencies are embedded in the one location to share intelligence, and more recently initiatives such as suspicious activity reporting (SAR) system have developed to improve the proactive detection and sharing of intelligence particularly on terrorism. Fusion centers and SAR systems are still evolving and are works in progress and will be examined more fully in Chapter 4. In addition to new initiatives, the events of 9/11 at the federal policing level resulted in significant resources and powers being given to the FBI, and deeper structural changes to the broader US intelligence community with the creation of the DHS in March 2003. The DHS for the first couple of years of operation looked like an agency in search of a purpose, however, in our discussion on the strategic management of the intelligence function in Chapter 6, we will see how this agency could play an important role in promoting better policing intelligence capabilities across federal, state and local agencies. The perceived failure of key US intelligence agencies such as the FBI and the CIA to detect and disrupt the 9//11 attacks also resulted in the Bush Administration giving them more powers to collect intelligence proactively with less oversight than before.

The significance of changes to post-9/11 US intelligence legislation will be discussed more fully in Chapter 7. However, the signing into law by President Bush of the bill called the 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism' (the Patriot Act) was a significant reversal of previous reforms that were codified in the Foreign Intelligence Surveillance Act (FISA), passed in 1978 and designed to safeguard against the recurrence of surveillance abuses as happened in the Hoover period

(Bazan 2007). However, civil liberty, privacy concerns and public perception that the US intelligence community after the 9/11 reforms was still doing a bad job, continued to raise concerns about the extension of powers to policing intelligence agencies, particularly the FBI (Hulnick 2004). As discussed later in Chapter 7, the Obama Administration has reviewed the earlier legislation and guidelines issued by the former Bush Administration for intelligence collection by the CIA and the FBI. It is probably too soon to predict the results of these reviews and their impact on policing intelligence more broadly in the USA.

In summary, the origins and functions of US policing intelligence were driven by a combination of factors. Again there are some themes familiar to other countries discussed in this Part. The greater uptake of technology and specialization in policing and intelligence methodologies has been important. However, there is also a combination of other events more unique to the USA that explains the development of policing intelligence there. For example, the large number of police services and the fragmented response to policing at the federal, state and local levels make the implementation of truly national approaches to intelligence practice like the UK NIM difficult. The significant and ongoing reform of policing intelligence post 9/11, particularly at the federal and regional levels, has seen the adoption of initiatives to better promote coordination and more proactive intelligence strategies between agencies. However, new initiatives need to be balanced against the US public's natural suspicion of police powers and the will of politicians and management to see the reforms through.

### *Australasian policing intelligence*

In comparison to the fragmented US policing intelligence response, Australia with its eight police forces and New Zealand with one national police force, might imply, due to the smaller size of each policing community, a more unified and common historical approach to policing intelligence in Australasia. However, the history and origins of policing intelligence in both countries suggest that even within the one agency, the New Zealand Police (NZP), there have been diverse approaches to policing intelligence from early days. Rivalries and distrust between different area commands of the NZP and between Australia's federal policing agency – the AFP – and its state policing counterparts resulted historically in different and uncoordinated approaches to intelligence. The origins and functions of Australasian policing intelligence are partly the result of factors seen elsewhere in the UK, Canada and the USA, but also reflect other unique historical 'local' influences. Again, Australasian policing intelligence practice has been influenced by the use of technology, the uptake of new policing models (e.g. community policing and problem-orientated policing) and responding to new public managerialism ideas. All of these have been important in shaping the development of Australasian policing, but given they have already been discussed, I will focus on those issues that have been unique to shaping policing intelligence capability in both Australia and New Zealand.

The first different characteristic that defined the policing intelligence of Australasia was the relative geographic isolation of Australia and New Zealand, which meant that external threats were few and internal ones were not complex. There was some early development of intelligence capabilities, for example. Finnane argues that in the case of Australia, most Australian police forces from 1880 to 1930 underwent refinements in their organizational structures. This refinement included the development of specialist roles including the increased capacity for intelligence, surveillance and forensic work (Finnane 1994: 31).

However, the isolation of Australia and New Zealand resulted in what Rogers refers to as a 'benign threat environment leading up to the end of the Second World War and some would argue three decades after it' (Rogers 2009: 14), which did not encourage the development of more sophisticated thinking about and application of intelligence in Australasian policing agencies. In other words, neither Australia nor New Zealand policing agencies were confronted with either the suite or complexity of terrorism, nationalist, organized crime and communist threats experienced by their UK and US policing counterparts. A similar trend emerged within New Zealand policing. In the beginning there was more than one police force in New Zealand, though earlier versions were regional or local in focus, and intelligence practice was rudimentary. The unification into one policing agency in 1886 resulted in greater rationalization of resources and also the ability for improvement in various policing specializations including intelligence.

However, in the 1970s, the changing threat environment overseas started to impact on the Australasian region and the introduction of illicit drugs and increased migration changed the nature of both countries as their criminal markets became more connected to global trends. In addition to a greater connection to global drug markets, Australia and New Zealand policing agencies became more concerned about terrorist attacks offshore. For Australia, Rogers argues that the attack by the Black September faction on the Israeli contingent at the Munich Olympics on 7 September 1972, and the detonation of an explosive device outside the Hilton Hotel in Sydney on 13 February 1978, during a Commonwealth Heads of Government Meeting, sharply refocused the attention of the federal and state level policing on their counter-terrorism capabilities.

After the 1978 Hilton Hotel bombing, two influential inquiries were initiated by the Australian federal government at the time: the Marks Inquiry, which reviewed current Commonwealth Law Enforcement arrangements (Marks 1978), and the first of what was to be two reviews by Justice Hope, which looked at Australia's protective security arrangements, particularly the relationships between the police services and the national security intelligence community (Hope 1979). Both the Marks and Hope inquiries were important early catalysts in building up the intelligence functions of Australian policing agencies. The Marks Inquiry was significant as it led to the establishment of the AFP in 1979. In just 30 years, the AFP's broad mission now includes a growing number of national and international issues such as counter-terrorism and organized crime to an even more diverse role of activities today including peacekeeping, high tech crime, money laundering and most recently war crime investigations. For the past decade, the AFP's role in

peacekeeping has been particularly interesting and Chapter 3 will focus in part on how it has been involved in building intelligence capacity in fragile South Pacific states.

In Australia, the 1980s and the 1990s saw several other independent reviews, which were not necessarily focused primarily on policing intelligence, but also impacted on how it was practised. There is insufficient space to provide full coverage on all of them. However, the federal government's review (the Costigan Commission in 1984) and the NSW state-based review (the Wood Royal Commission in 1997) were arguably the most important ones during this time. The Costigan Commission's review of corruption associated with maritime unions resulted in the creation of a federal organized crime body, the National Crime Authority (NCA), in 1984. The NCA was given strong coercive powers to collect intelligence and evidence to deal with organized crime. Although the NCA was abolished in 2003, and replaced by the Australian Crime Commission (ACC), the ACC has kept these coercive powers (see Chapter 7 for a discussion of these coercive powers). The ACC has recently developed a new approach to intelligence and I will come back to this in Chapter 4 as part of a broader discussion on new intelligence frameworks. The Wood Royal Commission in 1996 and 1997 into police corruption within the NSW Police also resulted in some internal restructuring of its intelligence capability (Wood 1997; Walsh 2005). Some of this reorganization resulted in an integrated crime management model, which was advocated by the UK intelligence-led policing model (the NIM ) as a best practice approach.

However, in Australia, the 1980s and 1990s continued to underline problems with the ways agencies conceptualized and used intelligence. In 1993, the Australian Government extensively reviewed via the Commonwealth Law Enforcement Arrangements Review (CLER) all aspects of Commonwealth (federal) law enforcement agencies' operations, including the performance of their intelligence functions. In particular, the report underlined a number of problems associated with intelligence practice, including tasking, coordination, analysis, collection and information management systems. The vulnerabilities detailed in the report relating to police information management systems worked against effective and proactive intelligence collection and analysis, which is meant to underpin contemporary intelligence-led policing practice (CLER 1984).

Many of the challenges to effective policing intelligence identified in the CLER Report almost two decades ago still exist. Subsequent chapters will address many of the challenges identified in further detail, but there also has been progress in some areas of policing intelligence practice in Australia. The growing threat from Sunni Islamic extremism, in particular the Al Qaeda 'brand', and other emerging transnational threats in the late 1990s such as maritime illegal immigration have resulted in further development of Australian policing intelligence capabilities. Additionally, in Australia in the late 1990s, there was growing evidence of the rhetoric of a 'whole of government approach' to policing and security issues being matched with reality. The AFP and other law enforcement agencies working in a tightly coordinated way with Australian national security agencies over maritime people smuggling from the late 1990s is a good example of a 'whole of government

approach' in practice. Another example of a growing coordinated and integrated approach to intelligence between federal, state policing and security agencies was the model used for intelligence support for the 2000 Olympic Games in Sydney. While multi-agency fused responses to large events are common now, in 2000 this response was unique and represented an effective way for national security and federal law enforcement agencies to coordinate their intelligence support to NSW Police who were providing security at Olympic venues in Sydney. The multi-agency police and security agency model adopted for the 2000 Olympic Games was also another important example of how normative change and new habits of cooperation and coordination could provide a template for further joint federal-state policing intelligence strategic and operational planning.

The late 1990s was also a period in Australian and NZ policing, when the influence of UK intelligence-led policing approaches started to be visible in the reform initiatives of local policing intelligence models. Chapter 4 will focus further on how UK policing intelligence approaches have impacted on the development of intelligence structures and processes in Australasia, the USA and Canada. Suffice it to say, the extent to which UK intelligence-led policing approaches have been adopted in Australian policing agencies has been uneven. In a study completed in 2005 of four Australian policing agencies (ACC, AFP, NSW Police and Victoria Police), it was clear that both at strategic and operational levels, further integration of intelligence policing strategies was required for intelligence to reach its potential of providing proactive support to decision-makers (Walsh 2005). The Ratcliffe review of NZP intelligence in 2002 also identified some of the same problems, and barriers to an effective intelligence-led policing approach in that agency, including variations in structure between intelligence units, poor data sets and a lack of integration of intelligence into decision-making processes (Ratcliffe 2002). The current reform agenda of NZP which will be discussed in Chapter 4 is addressing these and other deficiencies.

The events of 9/11 and subsequent policy initiatives in both Australia and New Zealand to broaden traditional approaches to national security to include other issues, such as organized crime, have also resulted in further specialization in policing intelligence capabilities of both countries. In addition to new counter-terrorism measures, which will be discussed further in Chapter 6, there have been recent attempts in Australia to bring the organized crime work done by the ACC further into the centre of national security policy-making circles. In New Zealand the recent creation in March 2009 of the National Intelligence Centre for New Zealand and the establishment in July 2008 of a specialized organized crime body, the Organised Financial Crime Agency of New Zealand (OFCANZ), resulted in greater policing intelligence capabilities for New Zealand and stronger coordination with its national security intelligence community. In summary, the strategic management, policy reform environment of security and policing intelligence has been very active in both Australia and New Zealand. However, unlike the USA, in both countries, there has not been a comprehensive attempt to restructure national policing and security arrangements. Similar to developments discussed earlier with UK, Canadian and US policing, the post-9/11 environment in Australia

and New Zealand has also resulted in the amendment or drafting of new laws, particularly counter-terrorism legislation. The impact of this new legislation on intelligence practice will be discussed further in Chapter 7.

## An evolving intelligence tradition?

Based on the historical development and application of intelligence in the traditional (conventional) environments of national security and policing discussed earlier, this last section explores whether it is possible to talk about an evolving *intelligence tradition*. Tradition is defined broadly here as a set of beliefs, customs, practices, principles and accumulated experience handed down from earlier generations of intelligence practitioners that inform contemporary practice. The discussion above of national security and policing intelligence suggests that to some extent a broad tradition made up of similar language, norms, cultures and approaches has emerged. The characteristics of this tradition discussed here not only help explain the historical development of intelligence. Articulating broad components of an intelligence tradition also assists in delineating the uniqueness of intelligence from other fields (e.g. psychology, criminology, strategic studies or economics), which, as will be discussed in Chapter 10, is important to progressing intelligence-related research and theory building. Additionally, a basic conceptual understanding of an intelligence tradition is also helpful in understanding how intelligence is being applied in new environments.

There are three characteristics which describe the intelligence tradition: *the security environment*, *secrecy* and *surveillance.* However, I expect some readers would, depending on how they define intelligence, argue for a greater or lesser number of characteristics. Just what intelligence is or is not remains contested among academics and practitioners. For example, one senior national security officer interviewed for this book suggested that much of policing intelligence was not really intelligence as it was not secretly obtained or privileged information. This comment suggests a narrow view both of what secret information is and therefore what constitutes intelligence. Other perspectives, such as Ratcliffe's 3-I model (Ratcliffe 2008) are helpful in explaining what intelligence does (interpret the environment, inform decision-making, impact on the environment). However, what I am proposing by introducing this phrase 'intelligence tradition' is to distil down into only a few characteristics what is meant by the *business* of intelligence. However incomplete this list of three characteristics may be, at the very least, these characteristics have been fundamental to defining historically what intelligence is, compared to other similar activities, such as research, data analysis, information collation and report writing.

### *The security environment*

The first characteristic that traditional approaches to intelligence have in common is the security environment. This environment may be different in some ways or similar in others, but the *raison d'être* for all intelligence is to provide

decision-making support for those whose responsibility it is to manage a security environment. At its most fundamental level, intelligence is about supporting decision-makers to risk manage their operating environments. As seen earlier, managing the risks in the security environment could involve understanding a range of risks and threats related to terrorism, criminal gangs or reducing fraud occurrences within a business. The intelligence function must not only interpret the security environment, but given resources are limited, the analysis it provides must make it easier for decision-makers to set priorities for dealing with the suite of risks that exist. The decision-makers' priorities hence become the intelligence function's collection and analytical priorities. However, through the generation of new intelligence systems and processes, autonomous from formal tasking and coordination mechanisms, the intelligence function is able to recalibrate decision-makers' priorities, or better still warn about an emerging risk that the decision-maker has no knowledge of. Since 1945, in all types of national security intelligence agencies, we have seen the development of more formal intelligence collection and priority systems, partly driven by external political tasking, but also internally as part of agency management processes. Chapter 4 will examine these developments in the context of discussing contemporary intelligence frameworks more broadly.

### *Secrecy*

Secrecy is the second but most important defining characteristic of this tradition. In earlier discussion about the origins of national security intelligence agencies, the very existence of many of them was kept secret from the public for decades. The history of MI6 is a good example of this preoccupation with secrecy; its existence was only officially admitted by UK PM John Major to the House of Commons on 6 May 1992 (Dorril 2001: 758). Historically, though not always in reality, intelligence has been defined by the ability to collect sensitive information without the target's knowledge. Secret intelligence collection is obviously important in order to provide decision-makers with forewarning about a target or a threat and its possible intentions. While the historical development of national security and policing intelligence shows an increasing reliance on open sources of intelligence, publicly available information sources on their own are not intelligence, and are not always sufficient to provide insights about a threat. The requirement to control secret information sources and collection methodologies has created by necessity a 'culture of secrecy' and this has become an important characteristic of the 'intelligence tradition'. The desire to collect secret information resulted in the development of closed information systems, and a 'culture of secrecy', where the 'need to know' principle governed distribution. However, the 'culture of secrecy' also resulted almost in a contradiction between sharing information with decision-makers or other stakeholders quickly, and closed information systems and practices protecting the information.

It would be incorrect, however, to suggest that closed secret information systems have prevented any sharing of tightly controlled information. As Herman notes, prior to 9/11 and its mantra of 'need to know', the current international intelligence

system had already evolved into what he refers to as 'a patchwork of bilateral and multilateral arrangements of all kinds and all degrees of intimacy'. Herman also suggests that information sharing arrangements were 'unusual in their secrecy, but in every other way they are not unlike other inter-governmental arrangements that have developed in other specialized areas of government' (1996: 204).

However, operational sensitivities, national interest and agency rivalries within intelligence communities very often meant that in reality not all information was shared even between 'friends'. Arguably, however, the changing security environment may pose the greatest challenge to the culture of secrecy, which defined the work of national security and policing agencies in the twentieth century. The necessity of global cooperation in responding to most transnational threats today, and the need for UK/USA Agreement agencies to collaborate in their intelligence activities with less traditional partners in Europe, the Middle East and elsewhere will challenge traditional notions of what should be kept secret and why. However, there is no doubt that the current scope and nature of transnational security threats have resulted in more flexible and arguably networked approaches requiring at least some of a cultural shift away from earlier hierarchical Cold War structures and attitudes of secrecy within contemporary intelligence agencies. At the very least, traditional intelligence agencies are having to adapt their cultures of secrecy in order to work more effectively with new tiers of government and non-government agencies, which are themselves increasingly becoming part of national intelligence communities.

### *Surveillance*

The third characteristic of the intelligence tradition is surveillance, which includes a number of related and inter-dependent activities, such as tasking, coordination, covert collection, analysis and decision-making support. Gill and Phythian argue that surveillance is a core concept to national security intelligence as '[it] helps generate knowledge in conditions of secrecy that can inform the formation and implementation of security policy; this is essentially a subset of the more general surveillance that constitutes contemporary governance' (2006: 29).

Clearly the increased global threat from terrorism, particularly since 9/11, means that there has been increase in surveillance by national security and policing intelligence agencies. Gill and Phythian are also correct in extending their definition of surveillance beyond national security and policing contexts. Surveillance is a common characteristic of all intelligence contexts, including within the private sector and the newer applications of intelligence discussed in Chapter 2. In the private industry context, for example, surveillance has many applications. Companies do 'spy' on each other and companies and governments spy on each other. For example, the 2009 case of the arrested Rio Tinto mining executive, Stern Hu, accused by the Chinese Government of spying and stealing state secrets by attempting to bribe Chinese steel companies over their steel prices (O'Sullivan 2009), and the German news service Deutsche Welle (23 May 2009) reported in 2009 that the security department of Germany's largest bank, Deutsche Bank, had

allegedly been spying on employees by putting bank managers under surveillance and also other people outside the financial institution. On a less dramatic level, private industry use business intelligence processes and technologies such as analytics to project future threats to their financial viability.

Surveillance need not necessarily be a technologically dominant activity, and, however applied (whether physical, technical or electronic), it has become the cornerstone for intelligence collection and analysis across the traditional areas of national security and policing intelligence. The potential real strength of any surveillance is to provide forewarning of a threat. The dramatic developments in technologies throughout the Cold War have facilitated greater volumes and more rapid collection of covert information than frequently can be analysed. For example, the US sigint agency – NSA – like other sigint agencies, is in a dilemma between what can be collected and analysed. Of course not everything that is collected should be analysed. Surveillance is only useful if the significance of the information is assessed quickly and given to the relevant decision-maker.

Since the 1970s, technology has again become partly the answer to large data sets, particularly those collected by electronic surveillance methods. New intelligence applications being developed in one area of intelligence are being taken up by other areas. Technological advancements in software used in the private and the military sectors are supporting better intelligence analysis across broader applications of traditional intelligence practice. There is now analytical software which can assist in generating hypotheses, collating data (both quantitative and qualitative), brain storming and data mining. Various cognitive analytical techniques such as alternative analysis used initially in military and national security intelligence are now being increasingly used in policing intelligence (see Chapter 8). Strategic analytical tools, first used in the private sector (particularly engineering and business), are now being used in national security and policing intelligence to assist in strategic or estimative intelligence.

In addition to a range of analytical software that supports analysis, other older analytical tools traditionally used in business intelligence are now being increasingly utilized in national security and policing contexts.

## Conclusion

This chapter provided a brief summary of the origins and functions of traditional areas of intelligence practice across Australia, Canada, New Zealand, the UK and the USA. Each country has developed intelligence agencies which reflect their own unique political and cultural environments. A broad analysis, however, of several factors across each country, including politics, bureaucratic cultures and the evolution of their security environments, suggests that there are many similarities between the national security and policing intelligence applications in these countries.

From this analysis, I would argue that a basic set of three characteristics has evolved into an ‘intelligence tradition’, which helps explain what intelligence uniquely is in these environments. It is likely that this ‘tradition’ will remain

important in defining intelligence in the traditional practice areas discussed in this chapter. In contrast, Chapter 2 will shift the focus from the traditional practice areas to how intelligence is being applied in newer areas. The focus will be on two emerging practice areas, the first, corrections, which have already used some intelligence capabilities in recent decades, the second, biosecurity, where the application of intelligence principles and processes are still emerging. Both Chapters 2 and 3 argue that intelligence scholars and practitioners have not yet adequately engaged in discussion about how intelligence can be usefully applied in a range of emerging areas, both to improve the collective response to problems in the security environment, but also to assist in the development of a discipline of intelligence.

# 2 Emerging intelligence practice areas

## Introduction

This chapter moves the focus from how intelligence has been applied in the traditional environments of national security and policing to 'emerging practice areas'. The phrase, 'emerging practice areas', could potentially have a number of different meanings. The term 'emerging' is also somewhat subjective and relative, in that what is considered 'emerging' for one observer may be defined as 'matured' for another. Nevertheless, despite a lack of precision in the phrase 'emerging practice areas', it is useful to describe an increasingly large number of public and private sector agencies, which are now developing intelligence capabilities to better inform decision-making. Emerging intelligence practice areas can also include agencies where intelligence is not a new addition to business processes, but can describe an environment where intelligence is not yet well coordinated or integrated into decision-making. Hence, the focus here is on practice areas in agencies, where intelligence is either relatively new and/or its application to tactical, operational and strategic decision-making remains under-developed compared to the traditional intelligence practice areas discussed in Chapter 1.

In the public sector, there is an endless list of agencies, which could be considered as having emerging intelligence capabilities. These include agencies with border protection functions such as immigration and customs, but also others with compliance and regulatory mandates in areas such as taxation, social security, securities, superannuation and anti-money laundering. The list of public sector emerging practice areas could also be extended to include corrections, juvenile justice and child protection. Examples in the private sector could include intelligence capabilities currently being developed in many large multinational companies in a range of business sectors: finance, mining, building, consumer services, biopharmaceuticals and utilities.

The significance of current developments in many emerging intelligence practice areas is still not fully understood by those working in the traditional areas of national security and policing. I argue in this chapter that, given the increasingly complex security environment, a greater understanding by those working in the traditional intelligence areas is needed on how intelligence capabilities are developing in emerging practice areas. In the past decade in particular, countering

sophisticated terrorism and organized crime has required national security and policing agencies to work more closely in extended intelligence networks. These networks have included the specialized capabilities of regulatory and compliance agencies, particularly those working in tracking money flows, social security, corrections and immigration. Additionally, the private sector has become linked increasingly with public sector intelligence networks through areas such as fraud, identity theft, aviation security and critical infrastructure protection. The net effect of the widening of the security agenda means traditional intelligence providers in policing and national security are by necessity becoming 'networked' with a range of public and private sector agencies with whom in the past they would have limited or no interaction at all.

However, despite current efforts in Australia, Canada, New Zealand, the UK and the USA to link with a range of agencies with emerging intelligence capabilities, little is known about the nature of intelligence practice in these non-traditional practice areas. This is a vulnerability for both practitioners and academics seeking better practice across the wider intelligence spectrum. In particular, there are three important questions about emerging intelligence practice areas that remain unanswered in the current research. First, how has the increasingly complex and expanding security environment impacted on the development of intelligence capabilities in emerging practice areas? Second, how has the interaction with traditional intelligence players working on a range of 'whole of government' or 'all hazard' security issues influenced the type of intelligence frameworks and systems adopted in emerging practice agencies? Third, to what extent are emerging intelligence capabilities in emerging areas good practice?

Given the increasing number of public and private sector agencies that are now developing intelligence capabilities, this chapter will examine these three questions by focusing on two emerging practice areas (corrections and biosecurity). Both these areas provide good illustrations of how intelligence capabilities are developing in non-traditional security areas. The existence of intelligence capabilities across the corrections sector is clearly not new, however, in many respects, 'corrections intelligence' conforms to the broader definition described earlier of an emerging intelligence practice area. While progress is being made, it is clear from the discussion below that intelligence practice in the corrections sectors of Australia, Canada, New Zealand, the UK and the USA is still developmental. In particular, the outputs of intelligence in the corrections sector have not yet been sufficiently integrated into decision-making. I have selected corrections as the first emerging practice area to study in this chapter as recent progress in developing intelligence capabilities still, in most cases, requires more consolidation in each country. Additionally, as noted below, it is important to identify where the challenges remain to improve correctional intelligence practice, given the increased importance of linking this kind of intelligence with that collected by policing agencies in areas such as organized crime and terrorism. In contrast, the second example of emerging intelligence practice areas – the use of intelligence in biosecurity – is still relatively new. The need, however, for the

effective application of intelligence practices by health and national security authorities in these countries to monitor and respond to epidemics, and potential bioterrorism is becoming more relevant as countries develop broader definitions of national security and the knowledge of how health-related threat issues are interrelated.

## The corrections environment

Unsurprisingly, the correctional environments in Australia, Canada, New Zealand, the UK and the USA differ in a number of ways. To some extent, the differences are similar to those discussed earlier in Chapter 1, in the context of their national security and policing agencies. For example, variations in each country's political cultures and criminal justice arrangements have resulted in different responses to corrections policy. In the USA, for example, the corrections sector consists of federal and state prisons, while in Australia responsibilities for prisons remain with state governments. For Australia, this means that people charged with federal offences such as terrorism are held in custody in state prisons. The history and variations between the corrections sector of each country are documented by Cavadino and Dignan (2006) and Weiss and South (1998). Relevant to the development of intelligence capabilities in corrections are changes in the security environment that required correctional facilities to either establish or enhance existing intelligence capabilities. Correctional managers are requiring more support from their intelligence staff, more than just the traditional role of helping to risk manage offenders posing threats to prison staff and other offenders.

The question is, what has caused corrections administrators and facility managers to recalibrate the expectations they have of their intelligence capabilities? It is beyond the scope of this chapter to provide a detailed account of all the changes in the security environment which have impacted on the development of intelligence capabilities in prisons. Instead, I will focus on two priority areas: gangs and terrorism.

### *Gangs*

In the USA, since the early 1950s, there has been a steady increase in the numbers of gangs in major cities such as Los Angeles, Chicago, Cleveland, Denver and St Louis. It is clear that in most of these major US cities, county and state jails have had some semblance of gang intelligence units for decades. In this section, however, I will focus on how intelligence has been applied to the gang problem in the Los Angeles County jail system where the threat was recognized early. The perspectives here on gangs in the Los Angeles correctional environment draw on relevant literature, and also an interview I conducted in 2009 with Deputy Sheriff, Ramon Munoz, who works in the Operation Safe Jails (OSJ) Unit for the Los Angeles Sheriff's Department (LASD). In Los Angeles, a gang intelligence unit

was informally in existence in 1986, although it was not officially recognized until 1990, when it became known as the OSJ unit. It is responsible for monitoring the activities of in-custody street gang members, prison gang members and other disruptive groups within the county jail system.

The OSJ unit was created initially to build a nexus between what was occurring on the street and who was 'calling the shots' from the county jail. This wealth of intelligence has been invaluable to detectives and the district attorneys prosecuting crime on the outside. Across the rest of California, and the USA, many county jails have followed the Los Angeles County OSJ approach. For example, the San Diego County Sheriff's Department and Las Vegas Sheriff's Department officials have been liaising with the LASD, and are now in the process of launching similar OSJ programmes using their existing gang intelligence operations units. The scope of the 'gang problem' in the US corrections system spurred the creation of intelligence activities such as the OSJ. Concerns about the growing threat of gangs have also driven change in the prison sectors of other countries.

On a different scale, in New Zealand, Prison Services National Intelligence Manager, Rick McKee suggests that dealing with gang members in custody was also one of the main drivers for prison services developing an intelligence capability. New Zealand Prison Services data suggest that 24.5 per cent of the prison population are gang members, though McKee estimates the actual number is likely to be some 10 per cent higher. Overall, this is a high number but he said it also reflects the criminal environment outside in the community (interview, 10 March 2010).

Concerns about gangs have been one driver for the development of more effective intelligence capabilities in UK prisons, but not necessarily the main one. Other factors have also been influential, including a growing focus by corrections security and intelligence officers on organized crime groups and radicalization. One senior officer from the UK National Offender Management Service (NOMS) has suggested that it was a convergence of both these issues and others, including violence, drugs and obviously escape risk, which has driven improvements in intelligence capabilities in UK prisons. In a 2008 workshop on gangs and drugs hosted by the Correctional Service Canada (CSC), a senior manager of the UK NOMS said the gangs 'were emerging but not significant' (Wheatley, cited in CSC 2008: 17). There is also little available research that provides sufficient evidence of the 'gang problem' in UK prisons – whether they are a continuum of street gangs or form in prisons is not clear (Wood and Adler 2001).

Similar to the UK situation, it is also unclear to what extent a perceived gang problem in prisons in Canada and Australia has been the major catalyst for recent enhancements in correctional intelligence capabilities. However, in the case of Canada, it is obvious from recent CSC reports that gangs, particularly outlaw motorcycle gangs and aboriginal groups, are an increasing concern generally to correctional facilities. A 2009 *CSC Research Plan* identifies gangs and organized crime as a major strategic research priority (CSC 2009: 19). The CSC's 2008 Annual Report also reports on improvements being made in the development of

security intelligence networks to support security intelligence officers to deal with gangs inside Canadian correctional facilities (CSC 2008: 42). Whether a growing gang problem in the Australian correctional environment has driven improvements in intelligence capabilities is less certain. In Australia, gangs in general remain under-defined and under-researched.

Despite variations in how the threat from gangs is assessed across the different countries discussed above, the increasing imprisonment of gang members and the need to manage gangs that form inside prisons have resulted in the requirement to risk manage the prison environment to ensure the safety of both inmates and staff. The USA and particularly large cities such as Los Angeles have been using intelligence for some time to assist in risk managing the growing gang problem in Los Angeles County. The risk of gang-related violence and crime in this one county jail system is high. Deputy Sheriff Munoz in an interview described the risk posed by a diverse range of gangs to Los Angeles County in the following way:

> Los Angeles County is the gang capital of the world. LA County has over 120,000 documented gang members in its system. We have all sorts of drug cartels, organized mafias, street gangs, racist organizations, internationals and domestic terrorist groups living behind our bars. No other county in California or even the United States has the melting pot that Los Angeles has.
>
> (interview, 11 March 2010)

In response to the threat posed by gangs in custody and in the community, enhanced attempts to collect intelligence in the corrections sectors of Australia, Canada, New Zealand, the UK and the USA have been made, including criminal history checks and close liaison with policing agencies. This information has facilitated a greater understanding of gang activity and a more effective separation and management of rival gangs who may incite violence. For example, in the Los Angeles County jail system and in other US prisons, classification units frequently do the initial separation of violent inmates from the lower security level inmates. Many of these units also act as intelligence units. The interception of communication (telephone and letters), surveillance and, in some prisons, the collection of covert information from informants or undercover officers, have also produced greater strategic and operational knowledge about the risks posed by gangs in US prisons.

Like the USA, UK prisons also use interception of communications and covert human intelligence sources (CHIS). There has also been an increased emphasis in recent years in the UK prisons on working more closely with policing agencies in sharing intelligence. All UK prisons have an identified police secondee to assist in joint working, which includes sharing of intelligence and operational activity. There are also networks with other law enforcement agencies such as, for example, Special Branch and, increasingly, SOCA. While an increasing amount of intelligence is being collected in UK prisons and shared with external agencies, some correctional intelligence staff have suggested that police intelligence is still

not routinely shared with prisons. Practitioners I talked to suggested this was particularly important when police intelligence related to prison safety and security.

In addition to the above-mentioned collection methodologies, Prison Services in New Zealand also use what McKee refers to as 'intelligence-led searches', trust account analysis and 'RAT chats' or Routine Activity Theory interviews (interview, 10 March 2010). Additionally, deputies working in Los Angeles County jails collect intelligence by deciphering 'KITES' or notes, messages and letters that prisoners write.

New Zealand prisons have also developed various analytical products which are orientated specifically around gangs and gang members. These include 'subject profiles' (used to identify and provide recommendations against targeting specific members' centre of gravity and critical vulnerabilities), 'knowledge profiles' (which describe a specific gang's organization, *modus operandi* and links) and 'problem profiles' (which describe the specific criminal behaviours attributed to gangs and responses to these). Similar intelligence products are produced in the UK, Canadian and Australian correctional agencies. In addition to the kinds of gang-related intelligence products mentioned already, Munoz from LASD also described other additional products that are interesting: including 'imagery analysis' on baseball cards and tattoo decryption (interview, 11 March 2010).

### *Terrorism*

In addition to dealing with a growing gang problem in prisons, the intelligence capabilities of correctional facilities are also being challenged by managing individuals with radical Islamic views, or those who have become radicalized while in prison. The conversion of prisoners to Islam and other religions while in prison is not remarkable and many long-term prisoners do so, motivated by protection, redemption or seeking a sense of belonging (Hamm 2009). However, since 9/11, there has been greater policy and research attention on prison radicalization and its link to terrorism. Understanding the process of radicalization of Islamic jihadists in the community is difficult enough. It remains a greater challenge to accurately assess the nature of the links between conversion, radicalization and terrorism in prisons. This has been due to a combination of things including relatively low sentence rates for newly prescribed terrorist offences and a lack of focus on radicalization and terrorism by custodial facilities. It is also only recent that a more evidence-based research approach has been adopted in the US and UK prison systems to better understand the links between radicalization and terrorist activity (see e.g. RAND 2008; Spalek and El Hassan 2007; Hamm 2009). Hamm's two-year study of prison radicalization in US prisons provides some evidence of how charismatic jihadists, such as Kevin James, a 26-year-old Black Muslim from South Central Los Angeles, can adopt the beliefs and terrorist tactics of Al Qaeda. In 2005, the FBI foiled a plot organized by James' radical prison Islamic gang, Jam'iyyat Ul-Islam Is-Saheed (JIS) (or the Assembly of Authentic Islam), which

involved using a newly converted and radicalized parolee to attack US military sites and synagogues in the Los Angeles area (Hamm 2009: 668).

In the UK and the USA, since 9/11 there have also been well-known cases of individuals who have become radicalized in prison, including Richard Reid, 'the shoe bomber', and Jose Padilla. In more recent years, the nature of the potential threat posed by terrorism within correctional environments within the UK and the USA, in particular, has changed due to the increased incarceration of radical Islamic jihadists convicted of new terrorist offences in these countries. With an increasing number of jihadists in custody, there are obviously concerns in the corrections sector that these individuals will radicalize and recruit other offenders to extremist Islamic groups. It is important, of course, not to view the issue of radicalization as an intelligence collection and analytical priority for all prisons. There is a concern, however, that for many correctional intelligence officers and other staff, the lack of experience in handling individuals charged with terrorism offences will make it difficult for them to assess the threat such individuals pose to radicalizing other inmates. In addition to a lack of exposure to terrorist offenders, lack of knowledge about the drivers for radicalization, or Islamic society in general, also makes it difficult for intelligence officers to assess indicators for radicalization or the planning of terrorist activity. At the Los Angeles County jail level, Deputy Sheriff Munoz suggested that few deputies are familiar with Islamic and jihadist issues for two reasons. First, county jail intelligence officers are not likely to have in their custody inmates convicted of terrorist offences. These offenders are likely to be sent to state or federal prisons. Second, in Los Angeles County those inmates converting to Islam, who subsequently become radicalized, are likely to do so in state prisons where they are sentenced for longer periods (1–20 plus years) (interview, 11 March 2010). However, it is possible that individuals could become radicalized in the county jail system, but there is little awareness by correctional intelligence officers or research being conducted on which indicators may show this is happening. Munoz in his interview suggested that there was evidence in Los Angeles that some gang members are converting to Islam in US jails. He noted that inmates are meshing traditional Islam, 'prison Islam' and Western Islam (Nation of Islam) all together, though it is less clear why they are converting.

This blurring of gang affiliations with radical Islamic identity at the county level will require US correctional officers to develop greater situational awareness of the motivations and signs that gang members are becoming radicalized by extremist Islamic philosophies, and disseminate this information to the FBI, state and county police. The weak link in our knowledge about the potential threat posed by terrorism may not come from those convicted of serious offences, who will serve life sentences, but those who become radicalized serving shorter periods, who are then released back into the community. There have already been examples of individuals becoming radicalized during shorter sentencing periods, such as Kevin Gardner, who converted to extremism during his stay at a young offenders institution in the UK in 2006–2007 (ICSR 2010: 27). What the literature shows is that gauging the extent of radicalization in prisons remains unclear. The International Centre for the Study of Radicalisation and Political Violence's (ICSR)

study of radicalization in 15 countries, entitled *Prisons and Terrorism*, and Hamm's research noted earlier, are a step forward, but challenges remain in mapping the extent of radicalization and how to maximize the role of intelligence in monitoring such activity (ICSR 2010; Hamm 2009: 677).

## Corrections intelligence capabilities

The above provides a sketch of how some correctional agencies have developed intelligence capabilities to deal with the threats of gangs and terrorism. It is not possible to generalize from these observations as they are not in any way a representative sample of all developments in corrections intelligence across all agencies in Australia, Canada, New Zealand, the UK and the USA. A detailed understanding of the correction intelligence capabilities is complicated by a number of factors. First, gaining access to agencies to discuss their capabilities even in a general sense is difficult. Second, based on the small number of interviews I conducted with correctional officers, understanding intelligence capabilities is also limited by different views held by them on what intelligence is. Third, variations in the development of capabilities across agencies in the one country, and the size of many corrections communities make it difficult to gain any comprehensive understanding of the entire corrections intelligence sector. However, what is clear is that for many corrections agencies both the experience of having to deal increasingly with gangs, and now offenders in custody for terrorist offences, have become catalysts for improving intelligence capabilities. Managing the gangs problem particularly in the US correctional system, but also in Canada and New Zealand, has resulted in the development of better information (case) management systems for recording data and intelligence, the development of more systematic collection processes and the movement to link 'intelligence products' more to strategic and operational decision-making.

Such actions, though important to improving intelligence collection, will not amount to much unless they can be met by equal progress in analytical capabilities within the corrections sector. Again it would be inaccurate to over-generalize this point, but based on discussions I had with correction intelligence managers in Australia, New Zealand, Canada and the USA, the pace of development in the corrections analytical cadre remains slow. It was clear from these interviews that although civilian intelligence officers are being recruited to work in the corrections environment, prison officers still largely take on the role of 'intelligence officers' as an 'add-on' rather than being employed solely to work on intelligence. This means that in many correctional facilities intelligence collection and analysis are part-time activities, particularly in regional correctional facilities. A part-time and non-professionalized approach to corrections intelligence has consequences for the strategic, operational and tactical awareness of risks and threats in the prison environment. Additionally, the lack of relevant or quality training for corrections intelligence officers remains an issue in many correctional environments, though improvements in training are being made in some agencies across the countries discussed in this chapter.

Despite current deficiencies in capabilities, as noted earlier, a more challenging security environment (including complex gang networks and radicalized groups) has required correctional departments and facilities to develop a more sophisticated, strategic and operational response to applying intelligence. Corrections intelligence capabilities will always have a critical role in managing prison safety, but there is a sense now developing among a widening number of practitioners that it has other uses, including better prediction of potential threats and informing strategic decision-making. The priority of gang-related crime and terrorism in the security and criminal justice systems of the countries discussed here has also resulted in either the development or strengthening of various strategic arrangements between correctional facilities and state and federal policing agencies in these countries. Such relationships have provided operational support to policing operations, and also given correctional intelligence officers additional information about persons of interest within their facilities, who may be involved in illicit activity within or outside jail. The development now of more 'joined-up' approaches in some correctional intelligence environments with policing counterparts will continue to influence the ways prison managers develop their ideas about how to structure intelligence capabilities and what role intelligence plays in their prisons.

For example, in the USA, many fusion centers have become increasingly engaged with correctional intelligence officers due to concerns over prison radicalization. Some fusion centers have correctional intelligence officers seconded to them, while others have liaison arrangements or memoranda of understanding for sharing information. The inclusion of correctional intelligence officers in fusion centers is still relatively new, and it remains unclear to what extent corrections information is becoming efficiently integrated into such centers' operational intelligence priorities. In other non-US jurisdictions there are additional examples of loose or informal arrangements, where correctional facilities are not necessarily fused with policing agencies, but have other liaison arrangements and memoranda of understanding that define how intelligence can be shared.

As noted earlier, in the UK, SOCA works with the prison sector on organized crime issues. Corrections and police relations are also governed in many countries by specific legislation and regulations requiring corrections and agencies to share information. New Zealand Prison Services Intelligence Manager, Rick McKee described various acts governing relationships between prisons and various other agencies, including police, health, welfare, customs, immigration and inland revenue in New Zealand. However, in some Australian jurisdictions and in New Zealand, the level and quality of liaison between correctional and police intelligence officers vary. Some correctional officers I have talked to in recent years are frustrated by what they view as a level of mistrust between their agencies and their policing counterparts. This frustration is focused on what the police are prepared to share with them in return for information provided to police. In interviews in 2009, one senior corrections intelligence officer suggested that police mistrust in sharing their intelligence with correctional colleagues is a legacy issue relating to police perceptions of poor protection of information and sub-standard information systems in the corrections sector. However, the need for a 'whole of government' response to

terrorism, organized crime and gang issues will in time improve working relations, if not entirely extinguish the mistrust and organizational cultural attitudes each may have for the other.

The second question, posed at the start of the chapter, is to what extent interaction with traditional intelligence players such as national security or policing agencies has influenced the development of intelligence frameworks and systems in the corrections environment? Unfortunately, there is no clear answer to this question, as there is little research relating to this and other related correctional intelligence practice issues in most of the countries reviewed. Correctional intelligence officers and managers, particularly in the USA, have been frequent contributors to professional publications on intelligence matters (Garzarelli 2004; Buring *et al.* 2007). More recently, growing concerns about gang violence and terrorism are generating more evidence-based research approaches to correctional intelligence issues (Hamm 2009), but the output is low compared to other corrections research on topics such as suicide, mental health and addiction issues (Shoham *et al.* 2007). There may be a number of reasons for a lack of research in the public domain. First, as noted earlier, intelligence research potentially involves the investigation of systems and processes which are sensitive. The inappropriate dissemination of research that identifies specific vulnerabilities in correctional intelligence processes could jeopardize the safe operation of the facility being examined. The second reason may be the politicized environment in which many prison departments operate. This can result in overly risk-adverse executives not wanting to be seen to be exposing any shortcomings in the public arena.

Despite the dearth of current evidence-based research on the applications of intelligence in the corrections sector, in each country there is evidence of cross-fertilization of ideas, perspectives about intelligence doctrine, models, systems and processes being 'imported' from policing and other agencies. For example, in the Australian state of New South Wales (NSW), the Department of Corrections seconded a senior NSW Police officer to enhance its 'Corrections Intelligence Group' in 2004. Similarly, in New Zealand, Corrections Intelligence Manager Rick McKee originally came from NZP and prior to that had military intelligence experience in the New Zealand Army. McKee brought over from policing how to align strategically corrections to New Zealand Police so that both could operate as closely as possible. He has also applied to New Zealand prisons what he refers to as a 'diluted' version of the UK NIM. The UK NIM and other intelligence frameworks will be discussed in greater detail in Chapter 4. Additionally, in the LASD OSJ programme, deputies have worked already in a custody environment for a few years, and most also bring skills such as different languages, military intelligence experience or have a specific intimate knowledge of a gang. Based on discussions with some key UK prison officials, it seems that very few of their intelligence staff (or officers working within security departments of prisons) come from police backgrounds. There does seem to be some cross-pollination in training with UK prison intelligence staff learning from the police at a strategic level. The UK prison national intelligence model draws on police structures (e.g. $5 \times 5 \times 5$ evaluation), although one officer advised that there were not strong

parallels with the NIM, given the absence in the prison system of a strong level 2 structure (regional), as seen in the NIM for police. Despite a different approach to intelligence, the same officer suggested that there were broad similarities between the NIM and the prison national intelligence model, with the latter running monthly security meetings as a basis for tasking.

The answer to the third question raised earlier – the extent to which developments within corrections intelligence over the past decade in these countries represent good practice – again remains unclear. Interviews revealed some examples of good practice in some correctional environments in Australia, Canada, New Zealand, the UK and the USA. Further research is required to evaluate what constitutes good practice within and between these countries. What is clear from the interviews is that, for many correctional agencies, the development of comprehensive frameworks (that include effective collection and analytical capabilities), which in turn are integrated into decision-making across the sector, is uneven and in most cases a work in progress. Given the difficulty of doing intelligence research in the corrections sector, it may be some time until there is a greater willingness by agencies to trust researchers in evaluating aspects of practice. Research that is commissioned by correctional agencies may still come with heavy caveats, thereby reducing a broader scholarly understanding of effective corrections intelligence practice.

Notwithstanding the lack of publicly available evidence indicating where improvements are needed in corrections intelligence, some of the current barriers to better practice resemble those raised in debates (in the last decade) about the role of intelligence in policing. One common impediment in both intelligence contexts is the internal culture which undervalues intelligence. Managers need to demonstrate to the executive and other staff the *value* of intelligence. The National Manager for Intelligence for NZ Prisons identified cultural barriers as a major stumbling block, not just for the executive in his organization but also, ironically, for new intelligence staff in the correctional environment who were yet to be convinced of the need 'to do intelligence'. McKee summarizes well the dual challenges correctional intelligence managers face of creating the context and getting people to see the benefits of better intelligence practice, which may not be visible immediately:

> The hardest thing I have found, and what I think is the most important issue for intelligence (as people, processes and products), is the context or 'fit' of intelligence. Too many organizations like the sound of this 'intel thing' and simply bolt it on to what they already have and expect it to deliver results. This was like painting red an old car and expecting it to go faster. Intelligence works best when it has the right environment for it to work in. In corrections and in policing [in New Zealand] a few years ago, the environment was not quite right and much of my work is still less about intelligence and more about creating the context for it.
>
> (interview, 10 March 2010)

Beyond these challenges a more effective fusion is needed of corrections intelligence into policing intelligence in areas such as counter-terrorism and organized crime. The increasing number of individuals incarcerated for terrorism offences will require more systematic and formalized approaches to the collection and analysis of corrections intelligence which is in sync with external stakeholders' priorities. In the USA, efforts are being made by the corrections intelligence sector to be more integrated with external agencies on counter-terrorism and other crime issues.

For example, the FBI and the Bureau of Prisons have been working to link county corrections intelligence to federal task force arrangements such as the Joint Terrorism Task Force (JTTF). At the federal level, there are over 100 JTTFs which feed into a National Joint Terrorism Task Force (NJTTF). At the NJTTF, corrections intelligence related to terrorism from the local level can be assembled to provide a more accurate national picture of terrorism and radicalization in prisons. The NJTTF has also developed the correctional intelligence initiative (CII) to prevent potential acts of terrorism by offenders in US prisons.

The CII is led by a Bureau of Prisons secondee to the NJTTF. The CII monitors and counters radicalization and recruitment of offenders by extremist organizations and individuals. It is through the NJTTF network and other outreach programmes that Department of Justice Bureau of Prisons and the FBI outreach and engage with correctional intelligence officers at state prisons and county jails. However, despite these federal top-down arrangements, it is unclear the extent to which local information is linked up in real-time communication with federal agencies. Using Los Angeles County as an example, while the LASD is part of the local fusion center (the Joint Regional Intelligence Center (JRIC)), it is unclear the extent to which they are liaising on terrorist or gang-related issues with their fellow deputies in county jails. It is also not clear how federal intelligence collection priorities or the recent SAR initiative (discussed in Chapter 6) drives collection at the county jail level.

Given signs of radicalization in some US prisons, there needs to be a better understanding among correctional intelligence officers of radical religious and political philosophies including militant and jihadist Islam. As noted earlier, it is not clear the extent to which correctional intelligence officers have knowledge of the signs of radicalization once someone converts in jail. More effective training and awareness of indicators towards radicalization and violence need to occur at the county, state and federal level. An understanding of radicalization, jihadist Islam and building intelligence frameworks to provide early detection of these will also be important in Australia, Canada, New Zealand and the UK. A greater willingness by correctional departments to support research projects that can both evaluate intelligence officers' understanding of emerging threats and offer recommendations for improving practice generally are critical to enhancing how intelligence can support decision-making in this environment.

## The biosecurity environment

Beyond the 'headlines' of counter-terrorism and organized crime, there are a range of other equally serious threats located on an ever broadening security agenda. Biosecurity-related issues are another good example of a series of threats that are found at the intersection of traditional interpretations of international and national security and the broader post-9/11 homeland security agenda.

The term 'biosecurity' is similar to 'intelligence' in that it too has different meanings depending on the audience. The current literature reflects the ambiguity and debate surrounding the term, and also impacts on how the range of issues that fall under this broad term are dealt with as far as national policy setting is concerned. In the USA, for example, the term biosecurity was originally meant to encompass activities that prevent the transmission of infectious diseases mainly in plants and animals, but more recently there has been a shift to include humans and public health. Baker provides a good survey of different definitional perspectives, arguing that it has been defined differently depending on whether it has been interpreted in terms of the pathway of attack, the source of the threat, the target or a combination of all three (Baker 2009: 122). Biosecurity has also been used interchangeably with biosafety. Both terms are obviously related, but biosafety does have a slightly different meaning which it is important to clarify here. Biosafety, according to the US Centers for Disease Control and Preventions' (CDC) *Biosafety in Microbiological and Biomedical Laboratories* , is '[the] discipline addressing the safe handling and containment of infectious micro-organisms and hazardous biological materials.' The CDC suggests that 'the principles of biosafety were first introduced in its 1984 first edition of *Biosafety in Microbiological and Biomedical Laboratories* and have carried through to the most current fifth edition' (CDC 2009: 1). These principles focus on the containment and risk assessment of harmful biological materials. In summary, biosafety is about containing and safe handling of infectious biological material in order to protect laboratory workers, the environment and the public from exposure to infectious micro-organisms that are handled and stored in the laboratory. It involves a risk assessment process to ensure appropriate safety equipment is utilized to prevent laboratory-based infections. The focus for biosafety is on the protection of the individual working with micro-organisms in the laboratory rather than the community.

In contrast to biosafety, 'biosecurity' is newer terminology, and first came into vogue in the past decade. The fifth edition (2009) of CDC's *Biosafety in Microbiological and Biomedical Laboratories* does not define biosecurity but states its objective is to 'prevent loss, theft or misuse of microorganisms, biological materials, and research-related information'. 'This is accomplished by limiting access to facilities, research materials and information' (CDC 2009: 105).

The CDC explanation of biosecurity is too narrowly focused on laboratories and their employees as the source of threats or those most likely impacted by them. Other definitions are also too narrow – focusing on either 'accidental contamination' or 'deliberate acts of bioterrorism', without considering other biocriminal activities (Ryan and Glarum 2008: 19). In simple terms, the aim of biosecurity is

to protect dangerous biological materials from *accidental or intentional release into the community or environment*. In other words, inherent to biosecurity is protecting *populations* of humans, animals and plants, as well as the environment rather than just the individual dealing safely with dangerous micro-organisms in a laboratory. The spread of micro-organisms could be of course by accident via a global epidemic or intentionally via a criminal or terrorist act.

Another potential difference between biosafety and biosecurity, is the latter involves the intentional release of dangerous micro-organisms which constitutes a criminal act. Someone who avoids declaring prescribed food items at the border, or a terrorist group who intentionally releases dangerous micro-organisms as a weapon against humans, plants, animals or the environment, both pose a biosecurity threat. In either scenario, intentional or unintentional (e.g. in the case of an epidemic), biosecurity involves the prevention, detection, assessment and response to biohazards on a community, national and global scale.

The focus in this section is to assess how emerging intelligence approaches are being applied in the national security and health sectors to deal with a range of biosecurity threats. These threats include those that are intentional (from 'weaponizing' dangerous biological material – bacteria, viruses and toxins), and others that are unintentional from a diverse range of pathogens that threaten the food supply and the environment. Given limited space, I will not focus on how intelligence support is provided to detecting or assessing the threat of biological weapons from states or rogue nations. The issue of state-based biological weapons programmes has been dealt with extensively elsewhere, for example, Christopher *et al.* (1997) and Alibek (1999) who provide a brief history of biological warfare programmes between the two principal Cold War protagonists, the USA and the former Soviet Union. In short, though, the USA, the UK and the former Soviet Union did develop a series of biological weapon programmes, which were very effective particularly in the 1960s and 1970s. Most of these were progressively terminated in the USA and the UK, however, the Soviets kept up their manufacture of biological weapons until the late 1990s when they reportedly destroyed their stocks (Ryan and Glarum 2008: 13).

Throughout the Cold War, the 1972 Biological and Toxin Weapons Convention (BWC) became the principal international instrument to attempt – although many would argue unsuccessfully – to ban the production and proliferation of biological weapons. The BWC always struggled to provide (like relevant conventions for nuclear proliferation) a suitable verification mechanism to monitor the destruction of agents, toxins, weapons and biotechnology required to make biological weapons. In 2001, efforts to improve the BWC's inspection and verification process stalled (Koblentz 2009).

After the Gulf War and leading up to the invasion of Iraq in 2003, diplomatic and intelligence attention shifted from residual WMD proliferation concerns between the USA and the former Soviet Union to the intentions and capabilities of rogue states and non-state actors. Although it is easy to lump the threat posed from each WMD source (nuclear, chemical or biological) together in the same acronym, the nature of the threat each poses is not the same. In each case there

are differences in the ease of their production, proliferation and detection by intelligence capabilities. The production of fissile material (uranium or plutonium), its enrichment beyond a certain weight and the sourcing of specialized production materials, such as gas centrifuges, have globally been more controlled between the five major nuclear powers (the USA, the UK, France, Russia and China). Leaving aside concerns about North Korean and Iranian nuclear proliferation, in contrast to producing biological weapons, the development of a nuclear bomb still remains technically more difficult. The enrichment of uranium beyond a certain quality and quantity more quickly focuses suspicions and inspections from outsiders than those weaponizing biological materials. In contrast, the production and transfer of micro-organisms and related biotechnology are an easier enterprise for states and non-state actors. Biological materials can be produced easily and cheaply in the normal context of bioresearch, and those with harmful intentions can cover their tracks by carrying out their activities covertly in a range of legal public or private laboratory sites.

The extent to which intelligence agencies are able to detect and disrupt biological weapons proliferation remains today just as challenging as it was during the Cold War. The transference of biotechnology from one state to another attracts less attention from authorities given the multi-use of biological substances and technology in pharmaceuticals and vaccine production. The establishment by the USA in 2003 of the Proliferation Security Initiative (PSI), which uses US and other like-minded countries' intelligence and military efforts to proactively counter WMD proliferation between rogue states and non-state actors, may be beneficial in reducing the threat of biological weapons proliferation. National security intelligence agencies may 'get lucky' at intercepting the odd ship, which is transporting suspicious biological material and biotechnology from or to a country of concern. But the probability of intercepting, for example, shipments of biological material from North Korea, which reportedly does have the ability to produce biological weapons (Gronvall *et al*. 2009: 437), is extremely low, given pathogens and the technology to weaponize them are already freely available in most countries. Additionally, only very small amounts of biological material may be required for a successful bio-attack somewhere – making it unlikely a ship will be 'packed to the rafters' with anthrax. The fact that biological materials and biotechnology are now also inherently linked to legitimate global research and trade questions the validity of traditional non-proliferation and counter-proliferation measures in biosecurity, such as the PSI.

Intercepting or detecting biological weapons relies of course on having actionable intelligence that can provide forewarning that a bioterror attack is being planned. However, the Director of the CIA, Leon Panetta, at his confirmation hearing underlined the difficulty for intelligence agencies in finding the 'tactical footprint' of any imminent operation involving biological weapons (Panetta, cited in O'Toole and Inglesby 2009: 2). Despite enhanced biosafety and security in public and commercial laboratories in many Western countries, very small amounts of micro-organisms can still be produced quickly and discreetly with legitimate dual use biotechnology in these environments. Alternatively, micro-organisms can

be produced in countries where biosafety and biosecurity standards and export regulations are weaker (e.g. North Korea, Iran and Syria). In contrast to nuclear and chemical weapons of mass destruction, where intelligence may be in a better position to warn ahead of time of a weapons programme or an attack, conventional intelligence collection strategies may not prove overly helpful in interdicting biological weapons, particularly in circumstances which do not require sophisticated ballistic launch programmes.

This difficulty in detecting the tactical launch of a 'bioterror weapon' also makes it challenging to assess accurately, with any confidence, what threat level is posed from different kinds of bioterrorism. As noted earlier, since 9/11, several concerns have been raised about the growing threat from bioterrorism (e.g. Brower and Chalk 2003; Gursky *et al.* 2003; O'Toole and Inglesby 2003). Such concerns are warranted by a number of incidents pre and post 9/11, which demonstrate the motivation of some groups, if not yet their capability to use biological weapons. For example, in the 2007 memoirs of George Tenet, the former Director of the CIA (*At the Center of the Storm*), Tenet mentions two individuals who were instrumental in Al Qaeda's attempts to develop a biological weapons capability. In 1999, Al Qaeda's Deputy Ayman al-Zawahiri recruited a Pakistani veterinarian Rauf Ahmad to establish a small biological weapon lab in Khandahar, Afghanistan. Apparently Ahmad's efforts were short-lived and he quit the operation reportedly over not being paid enough. The second individual, Yazid Sufaat, was a US-educated Malaysian biologist. Sufaat had isolated anthrax in a building in Khandahar, but it had not yet been weaponized. Both Ahmad and Sufaat were later arrested trying to flee Afghanistan in 2001 (Tenet 2007: 278–279). In 2002, incoming US forces destroyed Al Qaeda's bioweapons laboratories in Afghanistan. Although the labs were pre-operational, they demonstrated the ability of terrorist groups to adapt operational planning to bioterror rather than conventional attacks such as improvised explosive devices. A second worrying incident involved anthrax spores found in the US mail system. This attack turned out to be the actions of what the FBI believed to be a mentally unstable scientist, Bruce Ivins, who was working at the US Army Medical Research Institute of Infectious Diseases (USAMRIID) in Fort Detrick, Maryland. Ivins later committed suicide before being charged officially by the FBI in August 2008 (Mackenzie 2009). Although the attack killed only five people, it underlined to officials in the early days after 9/11 the vulnerability of the USA to other bioterror attacks.

While in a general sense, the threat from a potential bioterror attack exists, there are diverse assessments between scientists and intelligence experts on the capabilities of some terrorists groups to produce and 'launch' bioterror weapons of sufficient magnitude to kill hundreds of thousands of people. As noted earlier, the generally widespread availability of biological material occurring naturally in most countries, accompanied by cheaper communications, transportation and biotechnology globally makes the accessibility of biological material easier for terrorists who wish to use them. But accessibility does not necessarily mean easier weaponizing. In 1994, many years before the 2001 anthrax mail scare, the well-resourced and organized Japanese cult Aum Shinrikyo secured anthrax, botulinum toxin and

Q fever. They tried to release potentially deadly clouds of these biological substances at least a dozen times but were unsuccessful. In one instance, they used anthrax spores from the roof of a building in Tokyo, but they deployed a harmless strain used in veterinarian vaccines which had no effect on their human targets (Broad 1998). In March 1995, they turned instead to sarin gas – spraying it in the Tokyo subway – killing 12 people and injuring several thousand others.

The Aum Shinrikyo case illustrates that different bacteria and viruses have varying requirements for their production, storage and weaponizing, and these conditions must be met in order to safely produce sufficient amounts of the harmful micro-organisms required. A terrorist group could decide, for instance, to produce anthrax but first needs to source it. They could attempt to extract it from contaminated ground soil in areas where anthrax is endemic to cattle, or it could be sourced by a 'lone wolf sympathizer' working inside a usually highly controlled laboratory environment, or from an overseas supplier in the Middle East or Africa.

The terrorists would then need the services of a well-trained microbiologist who could adeptly and safely cultivate it. Biological weapons production obviously cannot be done in the same manner and conditions used by a group of people sitting around a kitchen table making a simple fertilizer bomb. Without a safe laboratory environment, with all the appropriate ventilation and barrier protections, the terrorists would kill themselves first before having the opportunity to launch their planned attack. Perhaps a well-resourced group, with the appropriate number of skilled biologists and technicians could cultivate anthrax, but the bacteria also needs to be freeze-dried, and most likely then rehydrated into an aerosol form for weaponizing. Weaponizing bacteria requires a scientist with additional technical skills beyond merely growing the culture. In any case both of these skills are not likely to be found necessarily in all microbiologists. The successful launching and dispersal of the biological weapon containing the anthrax also depend on selecting a delivery system that would ensure maximum exposure if the goal was multi-casualties.

Delivery of the weapon to the target also relies on wind, time of day, weather and atmospheric conditions, and perhaps ideally a cloudy day, given anthrax may quickly degrade in the sun as strong ultraviolet rays can degrade the bacteria's DNA. The point of the anthrax example is not to downplay the possibility that a terrorist group could produce and weaponize such a dangerous micro-organism. Rather, its intention is to highlight that it is not helpful to either overplay or underplay any specific biological weapon scenarios, without further intelligence and scientific analysis of the specific biological agent and the group showing intent to use it. It is clear that an operational decision by a terrorist group to go down the biological rather than conventional explosive weapons route throws up a number of additional logistical hurdles before a successful attack is possible. The conditions that will both constrain and facilitate the operational use of biological weapons need to be understood more across different bio-agents. In summary, a more sophisticated analysis of the risks and threats posed by specific biological agents and the groups that may wish to use them needs to occur.

Regardless of the level of uncertainty over the likelihood and capabilities of specific terrorists groups to carry out some kind of bioterror attack, there is at least

a political consensus by the Australian, Canadian, New Zealand, UK and US governments that the use of biological weapons in terrorist attacks remains a significant threat. For example, in the US ODNI public version of the *National Intelligence Strategy*, 'mission objective one' and 'two' articulate clearly the priority of WMD proliferation and countering violent extremists' use of such weapons (ODNI 2009a).

While the focus by those on bioterrorist threats has been on 'traditional' agents such as anthrax, smallpox and the plague, there is an almost endless list of harmful micro-organisms and toxins that could be used by terrorists. The attack may not of course be in the first instance against humans, but could result in the release of a toxin or invasive species (plants, pest and insects) to impact the food supply or environmental security. There is also a range of new potential types of bioterrorist threats such as terrorists possibly using new genomic data or 'DNA hacking' to exploit DNA sequence information (Carlson 2003; Hammond 2006). Scientists using synthetic genomics have been able to reassemble the polio virus, which disappeared naturally in the 1970s, and the extinct 1918 strain of the influenza virus which killed 20–40 million people globally. Biotechnological advancements will soon allow scientists to decode the DNA sequence of other microbes and even create new microbes. Such biotechnology has dual use applications for legitimate biomedical research, but could also be exploited by terrorist groups seeking to use a 'super-bug' that had been genetically engineered with no available vaccine to counter it.

In light of the earlier discussion of biosecurity's broader meaning than bioterror attacks, a number of unintentional threats which might still have an impact on human biological security are pertinent. Again, the potential list is extensive, but would include pandemics such as the severe acute respiratory syndrome (SARS) and H5N1 which have already posed threats to global health. Biosecurity threats also include viruses, bacterial and other epidemic or infectious diseases to animals such as foot and mouth disease, which occurred in UK cattle in 2001, and biological threats to plants and the environment, which have a direct or indirect impact on humans from both a health and economics perspective.

Under the broader interpretation of biosecurity discussed earlier, the ability of intelligence applied both in the health and security context to tactically assess the possibility of an imminent threat (intentional or unintentional) is unclear. It is not possible to 'lock out' all hazardous pathogens which are readily found in nature to combat terrorism or any other biosecurity threat. Terrorist groups have proved to be flexible in their operational methodologies and target selection. Global trade in food commodities (plants and animals) also poses significant quarantine risks to particular countries, but these risks in many cases cannot be totally contained given that nations rely on such trade for continued economic development. This wider interpretation of biosecurity also means that intelligence officials working across the national security, health, agricultural, fishery, quarantine and animal health areas contexts, need to plan for a range of threat scenarios that go beyond conventional traditional biosecurity threat scenarios, such as anthrax attacks from terrorists. Others need to be considered, that are a bit more 'left of centre', yet could be possibly even more devastating on a nation's food supply, biodiversity and economy than the classical intentional bioterror scenarios.

As noted earlier in our discussion of bioterrorism, unintentional epidemics can quickly become global pandemics, with little warning, and the role of tactical intelligence sources in detecting and containing 'disease hot spots' in human, animal and plant populations will remain a challenge. It will also not be easy to assess, at least at the start, whether an epidemic was an intentional act of a jihadist terrorist, a racial supremacist, a disgruntled former government employee or whether it is an unintentional health event. Biosurveillance will be crucial in detecting epidemiologically early tactical indicators of a disease outbreak, and also hopefully mapping the actions of any perpetrators. But it will remain extremely challenging, and frankly is unrealistic for domestic security and policing intelligence to provide sufficient tactical warning to disrupt or contain every biosecurity incident, particularly those which may have just become operationalized.

As noted earlier, the military development of offensive biological weapons in the UK, the USA and the former Soviet Union during the Cold War provided much of the initial focus by national security intelligence agencies on this threat type. During this period, the focus of agencies such as the CIA was on the production and export of biological weapons and biotechnology in the Soviet Union. However, estimating the USSR's biological weapons capability was always an inaccurate process for reasons discussed earlier (Gronvall *et al.* 2009: 437). The application of biological weapons in the military context also provided some of the earlier impetus for the development of research and analysis of biological security and public health issues in civilian laboratories that we see today. The work carried out, for example, by USAMRIID – the US military laboratory discussed above – in Maryland has the primary responsibility for providing US military personnel protection against biological threats in the battlefield. However, its research activities are dual use and also provide the non-military population with medical defences against potential biological weapons. This exchange of biomedical research between defence and civilian laboratories in the USA provided an early model for cooperation between other federal government agencies, such as traditional intelligence agencies like the FBI, and those working in health-related areas that work with 'intelligence' from an epidemiological perspective.

Since 9/11, the scale and intensity of cooperation between traditional intelligence agencies (national security and policing) and other non-traditional players (in this case, health, epidemiology, biomedicine), who in the past would not normally have had a seat at the national security table, have increased. In the biosecurity context, a number of influences have brought national security intelligence, the health and scientific communities together. As discussed earlier, the 2001 anthrax in the mail incident and other unintentional health threats such as the 2005 SARS outbreak and avian influenza all have national security implications. These incidents cannot be dealt with by health or security agencies alone. I would argue that global health issues have become more securitized as the result of these recent pandemics, and this has consequences for how health and intelligence agencies now interact (Enemark 2007: 1–25). Pandemics, of whatever cause, also underscore the need for traditional intelligence actors (national security and policing agencies), and emerging intelligence practice areas (epidemiologist and biomedical scientists), to

combine skills and capabilities in order to more effectively deal with a number of threat issues across the full biosecurity continuum.

In a sense, the 2001 anthrax spores in the mail incident became an early test case for how traditional intelligence agencies and those who use intelligence principles in a health or scientific context could work together on a biosecurity incident. The 2001 anthrax investigation brought policing and health intelligence workers closer together, with the FBI conducting a criminal investigation and the CDC conducting an epidemiological investigation. Tumin argues that these investigations in the FBI and CDC produced large amounts of information, though both agencies lacked protocols for 'sharing what they knew and distributing it correctly' (2007: 3). The anthrax mail threat investigation exposed the normal investigative challenges that 'traditional' security and law enforcement agencies such as the FBI face, but it also highlighted coordination and information management issues between law enforcement, health authorities (such as the CDC) and the scientific community. In summary, while the 2001 anthrax investigation highlighted challenges between agencies with a national security and others with a health focus, it represented, if not by design, an experiment on how such diverse agencies could collaborate during a biosecurity investigation.

The central question remains, however, to what extent are the evolving post-9/11 biosecurity arrangements in Australia, Canada, New Zealand, the UK and the USA fostering more effective and collaborative intelligence initiatives between traditional national security intelligence, health and scientific agencies? If intelligence is to play a role in the detection, prevention, disruption and response to biosecurity threats, intentional or otherwise, to what extent are good intelligence methodologies being applied in this context?

In the last section of this chapter, I summarize some of the key policy developments in biosecurity for these countries as they relate to answering this question. After a brief survey of recent biosecurity policy changes in each country, I will suggest some ways that current biosecurity arrangements might be better supported by the application of more effective and formalized intelligence methods and processes.

## Post-9/11 biosecurity policy arrangements

Space does not permit a detailed listing of all major biosecurity policy landmarks in Australia, Canada, New Zealand, the UK and the USA, so discussion will be restricted to how key policy developments have influenced attempts by traditional intelligence practitioners (policing and national security agencies) to connect with their counterparts in the biosecurity intelligence context. The discussion will show that each country has developed their own unique response to biosecurity issues, however, two broad commonalities are immediately apparent. First, as noted above, in all these countries, especially after 9/11, a broader view of what constitutes national security has emerged, and issues such as bioterrorism and pandemics have as a result become more securitized in the past decade. Second, in all these countries post 9/11, there has been a greater attempt to rationalize government

responses to biosecurity. Governments have gone about this rationalization differently, and for the most part it is too soon to provide any definitive evaluation as to whether they contribute to effective biosecurity in these states. In general, reforms in the UK, the USA and Canada have resulted in multi-agency response to dealing with various biosecurity threats and risks. In contrast, the New Zealand and Australian response has been an amalgamation of a series of previous agencies, which had different responsibilities for biosecurity into supra-agencies such as 'Biosecurity New Zealand' and 'Biosecurity Australia'.

### *Australia and New Zealand biosecurity policy*

A common strand in both countries is to have a single agency dealing with this issue – at least the animal and plant aspects of biosecurity. In Australia since the election of the Labor Government in 2007 there have been a series of major national security-related policy statements released. I will come back to these in Chapter 6, but arguably the most important of these was the Prime Minister's National Security Statement, released in 2008. The Statement was important in signifying an even greater 'whole of government' approach to national security – one which adopted an all hazards philosophy to security issues. A key deliverable from the Prime Minister's Statement was to have a broader national intelligence community than the usual traditional groups of agencies. An expanded intelligence community now includes others such as the AFP, the ACC and Customs and Border Protection. A widening of the national security community now allows a broader number of agencies to decide on nationally significant intelligence requirements for Australia via the new National Intelligence Coordination Committee (NICC) (see Chapter 6).

However, other than Customs, the significance of biosecurity issues has not been captured in any significant way in the wider NICC membership. For example, the Department of Health and Ageing and the Australian Quarantine Inspection Service (AQUIS, now part of the new supra-organization of Biosecurity Australia) are not members of the NICC. A quick way to remedy this would be to have a member of the peak national committee of expertise of biosecurity, the National Biosecurity Committee as a member of the NICC, and ensure Australia's domestic security intelligence agency, the Australian Security Intelligence Organisation (ASIO), is represented on the National Biosecurity Committee. ASIO, the Defence Intelligence Organisation (DIO) and AFP have some expertise on aspects of bioterrorism, however, these agencies cannot provide the relevant scientific and epidemiological analysis of various biothreats, and it this expertise which needs to be represented in senior forums such as the NICC. Current arrangements reduce the efficient decision-making about a range of biosecurity threats (terrorists and non-terrorist), which potentially impact on the economic, social, health, political and environment security of Australia.

There are two recent additional policy landmarks that may be influential in the longer term in the development of biosecurity arrangements in Australia, though the jury is out as to what impact they will have on how traditional intelligence agencies (national security and policing agencies), and those with 'intelligence-

like functions' in health, veterinary medicine, quarantine and biosecurity research can work closer together on a commonly understood biosecurity agenda. The first policy initiative is the Beale Report, *One Biosecurity: A Working Partnership* released in September 2008, which reviewed Australia's quarantine and biosecurity arrangements. The government had commissioned the review over concerns about the levels of cooperation and fragmentation between federal and state agencies responsible for various biosecurity activities. The review occurred against the backdrop of a few disease outbreaks in animals such as the Hendra virus outbreak (1994–2008) and equine influenza in 2007.

The Hendra virus was particularly concerning as it can be transmitted from its host (bats) to horses and then humans. Hendra virus incidents underscored deficiencies in Australian biosecurity arrangements, and the need for more collaborative connections between various experts dealing with different stages of a biosecurity threat. In the Hendra virus case, there needed to be better coordination and integration of expertise between those working on the virus, including wildlife biologists, vets and human disease specialists (Prowse *et al*. 2009).

The Beale Report is noteworthy in advocating Australia move away from a traditional isolationist defensive quarantine approach that tolerates no risk to a more realistic one in the age of globalization, which promotes a risk management approach pre-border, border and post-border. Beale was also noteworthy in recommending the development in Australia of one supra-institution that would pull together disparate agencies responsible for biosecurity. The report, however, makes scant reference to the role of intelligence in promoting better risk management of biosecurity, and there is only one reference to a new national biosecurity authority needing to work collaboratively with other relevant portfolios including police and intelligence agencies.

The focus of the report is squarely on quarantine, animal and plant biosecurity issues. There is no attempt, other than a passing reference, to examine how these issues are related to human biosecurity and bioterrorism issues (Beale 2008: 158). The final biosecurity policy initiative relevant here was the 2010 publication of the Australian Government's *Counter-Terrorism White Paper: Securing Australia – Protecting Our Community*. However, surprisingly, this report has no specific section on bioterrorism; these threats are dealt with superficially together with other WMD categories (chemical, radiological and nuclear weapons) (Department of Prime Minister and Cabinet 2010).

It is not certain when the recommendations of the Beale Report will be implemented fully. At the time of writing many of the recommendations were still being considered as part of the government's budgetary process. There is little publicly available detail also from the human health policy side of biosecurity. The Australian Government's Department of Health and Ageing simply states in its annual reporting cycle that it is 'working with its counterpart, the Department of Agriculture, Fisheries and Forestry to ensure human biosecurity aspects are "modernised and integrated" within the new holistic biosecurity approach that underpins the Beale Review' (Department of Health and Ageing 2009: 222). While Australia has an effective quarantine approach, it is still not clear how the disparate

policy initiatives discussed above will provide the country with the *one* national biosecurity approach, which can best risk manage a range of human, animal, plant and environment biosecurity threats. The current Biosecurity Services Group in Australia's Department of Agriculture, Fisheries and Forestry has a compliance and investigations area. There is also an area in the Department of Health and Ageing that deals with health security (particularly the regulation of sensitive biological agents that could be used for terrorist purposes). Though it is not at all clear whether both these areas have developed strong intelligence systems and processes that can assist in risk management decision-making for known or future threats across the entire biosecurity continuum. Recently the Australian Government funded an Australian Biosecurity Intelligence Network (ABIN) to enhance connectivity, information management and analysis between biosecurity agencies. However, the usefulness of the ABIN for sharing relevant time-sensitive biosecurity information among all stakeholders is unclear, given funding for this project is only for 18 months and the network mostly connects biosecurity scientists rather other stakeholders such as policy-makers.

Given the current arrangements, it also unclear whether the Department of Health and the Biosecurity Services Group have securitized their work and view their activities as having broader national security implications. Despite the recent rhetoric of a more all hazards approach to national security, the fractured policy response leaves one wondering whether the Australian intelligence community fully understands strategically and operationally the full range of biosecurity threats (intentional or otherwise) that could impact on the health and prosperity of Australia.

In 2003, the New Zealand Government went through a similar biosecurity review process to Australia which resulted in a new biosecurity strategy. Also, like Australia, the review resulted in the amalgamation of various agencies and functions into one new department, the Ministry of Agriculture and Fisheries Biosecurity New Zealand (MAFBNZ). The New Zealand biosecurity review, *Protect New Zealand: Biosecurity Strategy for New Zealand* (New Zealand Biosecurity Council 2003), was authored by the Biosecurity Council and identified in some respects similar capability vulnerabilities to those found in the Australian Beale Report. For example, the *Biosecurity Strategy for New Zealand*also referred to a fragmentation of biosecurity activities across several agencies, isolated silos of information and poor information sharing and systems (ibid.: 23). The report also highlighted that a more proactive approach was required in assessing threats and that current arrangements (in 2003), did not provide for strategic identification and management of risks. The report concluded that risk management had become increasingly reactive and this had escalated costs (ibid.: 23).

However, the strategy did not articulate how intelligence collection and analysis across New Zealand's biosecurity sector could create a better understanding of risks and threats at a tactical, operational and strategic level. The report was also very scant on how plant and animal biosecurity is linked or could be integrated better with the New Zealand Ministry of Health biosecurity responsibilities. Finally, although the report at the beginning clearly stated that its focus was not on bioterrorism, interestingly it did comment that 'conceptually bioterrorism is

simply another vector for transmission of unwanted pest and species' (ibid.: 7). Given this comment, it would have been useful for the authors to come to a conclusion if they saw a role for Biosecurity New Zealand in preventing bioterrorism through the transmission of such pests and species and what that role may be. However, it is also clear since the implementation of the 2003 Strategy, the new department – MAFBNZ – has progressed some intelligence initiatives to assist in developing a more proactive targeted approach to risks and threats particularly at the border. For example, since 2007, MAFBNZ intelligence staff have been co-located with other law enforcement intelligence officers based at the NZ Customs Service National Targeting Centre. These officers have been learning from Customs intelligence colleagues how to better profile biosecurity risks, including passengers arriving at air and seaports. This joining of biosecurity intelligence officers with Customs has also promoted better information sharing between agencies (Horton and Airs 2009: 7). The New Zealand academic and scientific community members such as the New Zealand Centre for Biosecurity and Infectious Diseases have also been active in the investigation, diagnosis and management of outbreaks of suspected infectious diseases. This centre highlights the importance of research in generating intelligence gathering on emerging diseases or other unusual or suspicious disease events. But again it is uncertain what links exist between this work and the collection and analysis on bioterrorism or biocrime threats by New Zealand's traditional policing (NZP) and key national security intelligence agency the New Zealand Security Intelligence Service (NZSIS). While the New Zealand Ministry of Health has portfolio responsibility for managing human diseases and pandemics, it is uncertain whether the new National Intelligence Centre at NZ Police Head Quarters, or the NZSIS run multi-agency Combined Threat Assessment Centre (CTAG), includes seconded specialist analysts, who could provide human or animal assessments on bioterrorism and other biosecurity threat issues.

The vulnerability of island countries such as Australia and New Zealand to the introduction of an exotic pest animal or plant, whether it was a terrorist, criminal or unintentional act, could easily threaten unprotected environments or unprotected primary industries. The net effect of such a scenario may be less compared in the short term to a terrorist group dispersing anthrax spores on the Sydney subway, but could do more damage in the long term if it impacted on the environment of the agricultural production of both countries. One estimate by Biosecurity New Zealand suggested a foot and mouth attack in that country would result in a 4 per cent drop in gross domestic product (GDP) in the first three months of the outbreak. After one year, it estimated that the cumulative loss in nominal GDP would be around NZD 6 billion (New Zealand Biosecurity Council 2003: 36).

Unlike Australia and New Zealand, the remaining countries (the UK, Canada and the USA) discussed below have multi-agency approaches to managing risks across their biosecurity sectors. Additionally, in contrast to Australia and New Zealand, the three countries share borders with others and in the case of the UK, multiple borders via the European Union.

***United Kingdom biosecurity policy changes***

In the UK, there are a number of government agencies that play a role in the country's biosecurity response at the national and local levels. In relation to the bioterrorism aspects of biosecurity, the Home Office leads the UK Government response and has a chemical, biolocial, radiological and nuclear (CBRN) team, and terrorism protection unit (with scientific seconders) to deal with bioterrorism issues. Several bioterrorism-related initiatives have come out of the Home Office Counter-terrorism Strategy, particularly in research, science, technology in the detection and management of biological incidents. In addition, the MI5-run JTAC now includes medical intelligence staff (Royal Society 2009: 5). Since 9/11, there have been changes at the Cabinet Office, which have brought enhanced levels of intelligence and policy coordination on all national security issues, including bioterrorism. For example, the establishment in 2001 of the Civil Contingencies Secretariat (CCS), which reports to the Prime Minister via the security and intelligence coordinator, was set up to improve the resilience of the central UK Government across a range of national security issues, including bioterrorism. 'Resilience' has become the core guiding principle for UK national emergency and contingency planning and has been defined by the Cabinet Office as 'the ability at every relevant level to detect, prevent and, if necessary, to handle and recover from disruptive challenges' (Cabinet Office 2003: 1). In March 2010, the Cabinet Office released further 'concept of operations' documents on how it would coordinate a response to a national emergency through its 'briefing rooms'. The March 2010 document lists pandemics such as H1N1 (swine flu) as one national emergency category that the Cabinet Office Briefing Rooms (COBR) would respond to (Cabinet Office 2003: 7).

Post 9/11, there have been also significant changes in the public health response to biosecurity issues in the UK. While the Department of Health provides 'resilience' in the prevention, control and treatment of infectious diseases, the Health Protection Agency (HPA) was created in 2003 to provide a more integrated response to protecting public health. The HPA has been established with functions that are not too dissimilar to the US CDC. It includes a number of important centres (the Communicable Disease Surveillance Centre, the Centre for Infections and the Centre for Emergency Preparedness and Response), which together provide important expert advice, early warning, investigation and response to accidental or deliberate threats to public health. The HPA's diagnostic and epidemiological expertise involves the use of 'health intelligence' techniques, with the establishment in 2004 of a medical intelligence unit, but it is not revealed if MI5 or policing officers are also part of the Agency's investigative team.

There are other policy players in UK biosecurity that stretch across other areas such as the Department for Environment, Food and Rural Affairs (DEFRA), which provides policy advice and some investigative capacity for controlling and managing the outbreak of diseases in the food supply, the environment and agriculture. However, again it is not revealed how animal health monitoring by DEFRA is integrated into policy responses to human health by the Department of

Health or the HPA. A 2009 Royal Society policy document argued that it 'was currently unclear which government department has overall responsibility for infectious diseases of both humans and animals at a policy level, and that a clear national policy is essential to achieve greater integration' (Royal Society 2009: 3). This suggests that despite the recent progress in the UK described above, there is not a single coordinated approach to biosecurity threats across the plant, animal and human health continuum. The UK fragmented response across all sectors of biosecurity is also common in the USA.

### *US biosecurity policy changes*

Both the UK and the USA share other similarities in biosecurity policy approaches. Since 9/11 each has created new national security and health security arrangements, increased funding for biosecurity research and even conducted joint exercises together such as 'TOPOFF 3'. However, both countries' policy prescriptions are different in other respects, reflecting differences in their political structure, geography, population and overall funding for bioterrorism and biosecurity issues. All these factors have impacted heavily on the ultimately different policy approaches between the UK and the USA (Jones 2005).

The US policy approach to biosecurity has evolved rapidly since 9/11. It is not germane to discussions here to describe in detail all the major changes in biosecurity policies since 2001. Instead in this section, I will describe briefly some of the legislative and presidential directives that have shaped current policy directions, and show how these initiatives have impacted on the relationship between traditional intelligence and emerging intelligence practice in health sectors. As noted in Chapter 1, almost immediately after the 9/11 attacks the Bush Administration created the DHS in 2002. The DHS mandate included becoming the lead agency for domestic management and coordination of federal operations to prepare for, respond to and recover from biological weapons attacks.

Following the establishment of the DHS, President Bush issued a number of Homeland Security Presidential Directives (HSPD), which further provided a policy 'blueprint' for biosecurity issues. Starting in 2002 with HSPD 4, *National Strategy to Combat Weapons of Mass Destruction* (DHS 2002), Bush outlined a strategy to combat WMD, although the document did not say much about biological threats or the broader suite of biosecurity threats. A later HSPD emphasized other aspects of biosecurity discussed earlier in this chapter. For example, HSPD 9, *Defense of United States Agriculture and Food*, (DHS 2004a), called for a national policy to defend the country's agriculture and food supply against accidental and intentional disease outbreaks.

While these earlier executive measures were important, HSPD 10, *Biosecurity for the 21st Century* (DHS 2004b), and HSPD 21, *Public Health and Medical Preparedness* (DHS 2007), arguably have resulted in the most comprehensive US Government efforts to counter bioterrorism and other biosecurity threats. HSPD 10 was critical in laying down the foundations of a national biodefence programme that included threat awareness, prevention and protection, surveillance

and detection and response and recovery. HSPD 10 in particular resulted in the establishment of three major initiatives: (1) the Biowatch Program (a network of environmental sensors to detect bioweapons attacks against major US cities); (2) Project Bioshield (a programme to accelerate the acquisition of medical counter-measures against bioweapons); and (3) the establishment of the National Biosurveillance Integration System (NBIS) (aimed at integrating human, animal and plant health surveillance information with food and environmental monitoring system and threat and intelligence information in real time). Another important measure was the creation of the National Biodefense Analysis and Countermeasures Center (NBACC), which does lab analysis to identify scientific underpinnings for current and future biological threat agents at Fort Detrick, Maryland.

HSPD 10 acknowledged that intelligence had an important role in enabling all these aspects of the national biodefence programme. However, the unclassified version of this document, at least, lacked any general comments about how intelligence could prevent or *disrupt* biological threats. The focus was more on how intelligence could play a role in responding to threats (DHS 2004b: press release).

HSPD 21 is also important in understanding US biosecurity approaches, as it established a strategy for public health and medical preparedness. Unlike HSPD 10, the focus is less on bioterrorism and more on providing a national approach to preparing US citizens against all kinds of potentially catastrophic health events. A big part of the strategy is the development of a national biosurveillance programme in order to better maintain situational awareness during a major health event. The directive is ambitious in that it seeks to engage government agencies at federal, state and local levels with academia and the private sector to respond effectively to a range of health incidents. Of particular relevance for national security and health intelligence agencies working closer together, the directive called for a 'national health security strategy'. The lessons learnt from the anthrax spore attack in the US mail system in 2001 in getting agencies with more traditional policing and security intelligence roles to work with those in the health sector have been progressed through HSPD 21, and subsequent initiatives such as the National Responses Framework.

However, despite progress being made between federal, state, local security and health services and the development of initiatives such as the 'National Response Plan', some biosecurity specialists have commented that the USA 'does not yet have a concept of operations or clear biosurveillance objectives' for such a plan. O'Toole and Inglesby argue that a 'concept of operations' is still needed that would 'map out how different levels of government, and critical private sector actors would respond to a bio-attack or to other public health emergencies of national significance'. They argue that a concept of operations is important in order to avoid a 'BioKatrina' (2009: 28).

Other researchers have welcomed the renewed policy emphasis on biosecurity, particularly the more 'whole of government' approaches emphasized through broad strategic statements such as HSPD 21. Nuzzo suggests that some headway has been made in implementing biosurveillance systems across the country, but the systems'

ability to provide real situational awareness during what she describes as catastrophic health events is uncertain, given there is no clear overarching national strategy for designing, testing, staffing, maintaining or funding such a system (Nuzzo 2009: 37). Nuzzo also suggests that:

> A workable concept of operations must underpin any effective national bio-surveillance system if multiple agencies and authorities in the federal government responsible for parts of biosecurity are able to develop an effective national surveillance capability. Such a capability needs to capture and coordinate not just public health emergency responses, but also must have a way to bring in the broader security agencies response to any national health crises.
>
> (ibid.: 37)

As noted earlier, the DHS at the federal level is at the centre of a range of bioterrorism and biosecurity initiatives. Given also the central role that the DHS is establishing in coordinating federal, state and local approaches to intelligence generally, it makes sense for it to take a leadership role in coordinating health and national security intelligence flows relating to biosecurity issues. However, it is clear from interviews conducted for this book in the USA that the DHS is still building its capacity to generate its own intelligence as well as act as broker for intelligence produced at regional and local levels. Therefore DHS's ability to effectively coordinate intelligence from local and state policing, health and emergency agencies in order to predict or provide accurate real-time situational awareness during a public health crisis intentional or otherwise remains questionable. This is not to suggest that DHS is not making further improvements in connecting national security and health intelligence at federal, regional and local levels. But there are challenges ahead that will impact on the USA and the abilities of other countries in building integrated nationally effective biosecurity responses which bring together the appropriate mix of national security, policing and health intelligence expertise at the appropriate time.

### *Canadian biosecurity policy responses*

Canadian biosecurity policy developments, like the USA, have been a multi-agency approach, though in contrast the pace of reform has been more incremental since 9/11. In Canada, the most recent significant biosecurity policy landmark was the release in October 2003 of the *National Advisory Committee Inquiry on SARS and Public Health* . This government-commissioned inquiry followed the SARS epidemic earlier that year, which by August 2003 had resulted in 44 deaths in the Toronto area. The report detailed a range of systemic deficiencies in Canadian public health including in information systems and sharing (Health Canada 2003: 1). The key recommendation of the National Advisory Committee report was that Canada needed a new national public health authority. This recommendation was implemented in 2004 with the establishment of the Public Health Agency of Canada. Within this new department a specialized area called the Canadian Centre

for Emergency Preparedness has the responsibility for centrally coordinating public health issues as they relate to disease outbreaks and health security-related matters such as bioterrorism. The Centre is broken down into additional sections, such as the Counter Terrorism Coordination and Health Information Networks which liaise with other stakeholders to raise awareness and provide early warning response surveillance to the health related aspects of WMD. The Centre also manages the Global Public Health Intelligence Network (GPHIN), which provides an early warning global surveillance website to disseminate real-time information to public health professionals worldwide on risk management, prevention, control and response measures. GPHIN was developed in 1998 by Health Canada in collaboration with the World Health Organization (WHO). It has extensive coverage in seven languages and its news reports comprise 40 per cent of WHO's verified diseases outbreaks (Hitchcock *et al*. 2007: 210).

Other more recent policy and legislative progress has been made in making the links between national security and biosecurity. In 2009, the Canadian Parliament passed the Human Pathogens and Toxins Act, which provides domestic oversight of pathogens and toxins including an inventory of who possesses them, and assessments on how safely they are being stored to prevent their deliberate or accidental release. And, additionally, from a policy perspective Canada's Chief Public Health Officer spoke of a 'one health' approach, which suggests a desire to connect the plant, animal and human dimensions of biosecurity.

Though this is encouraging rhetoric, it is not revealed how these connections are being forged from a policy perspective on the ground. It is not clear how Public Health Canada health intelligence networks are securitizing potential biosecurity threats, nor whether CSIS or the RCMP is using this information to respond and predict health threats, which may be deliberately released into the community. A glance at the membership list of the CSIS-run Integrated Threat Assessment Centre (ITAC) suggests that Public Health Canada is not a partner agency within the Centre. It is possible that Public Health Canada may provide input into health security-related threat assessments, but a more integrated and strategic relationship between national security and health intelligence issues could be achieved by an appropriately cleared health officer being embedded in the ITAC. Additionally, more strategic and proactive working relationships between the scientific, national security and health communities over biosecurity will be required in the future if the government wishes to articulate a common vision for biosecurity. The Council of Canadian Academies may be the appropriate body to draft such a vision for the government.

## Towards a more effective biosecurity intelligence approach

Based on the discussion above of biosecurity policy developments in Australia, Canada, New Zealand, the UK and the USA, it is clear that each country has developed their own policy prescriptions to this issue. Despite some of the differences, three common themes in each country can be identified, which underline the current challenges each face in building effective biosecurity

intelligence capabilities. In particular, each of the themes shows that both traditional intelligence practice (policing and national security) and health intelligence agencies could do more collaboratively to detect and respond to a range of biosecurity threats.

The first challenge is, how can governments get beyond their current fragmented approach to biosecurity? The USA and the UK have the most fragmented policy response with the creation of new agencies and coordinating bodies, however, even in Australia and New Zealand there are still multiple agencies across the biosecurity sector responsible for a range of plant, animal and human health threats. Much work has been done on reforming different parts of the biosecurity spectrum – plants, animals and humans – yet less on how to integrate these reforms more effectively to produce holistic biosecurity strategies. This remains a concern in all of the five countries examined, and the impact of this fragmented policy and intelligence space is evident in recent disease outbreaks, which were not identified early or crossed animals to humans, causing death. Recent epidemics such as the Hendra virus and avian influenza are examples of zoonotic diseases that can only be effectively dealt with if scientists and others working across different components of the biosecurity spectrum collaborate on mutually understood national biosecurity priorities. Some scientists and policy-makers in the biosecurity area have started talking about a 'one health' approach (Prowse *et al.* 2009) to biosecurity, yet as noted earlier it is still too early to know whether governments are moving beyond such rhetoric in practical terms. In general, there needs to be a much stronger link to establishing biosurveillance and biosecurity intelligence goals with the broader national security priorities, and this needs to be managed at the central national intelligence coordinating level. So in each country discussed, whether it occurs in the contexts of central coordinating mechanisms such as the ODNI in the USA or the Joint Intelligence Committee (JIC) in the UK, more consideration needs to be given at the senior executive intelligence coordinating level in governments to biosecurity threats. In an increasingly 'all hazards' approach to national security, central government intelligence coordinating bodies need to provide a clearer guidance to political decision-makers of what the key intelligence collection priorities are for *all* 'biosecurity intelligence' related issues not just bioterrorism. This will require individual members of the intelligence community, and intelligence priority setting committees to look across the entire biosecurity spectrum, and assess how threats in one area may be related in other areas. The setting of biosecurity intelligence collection priorities will also require an integrated approach to biosurveillance across different contexts, including some areas that may have previously not been thought of as relevant to national security, policing and defence, including environment, fish and wildlife, agribusiness, public health, biotechnology, clinical areas and related research.

The second challenge to building a more effective biosecurity intelligence approach relates to human resources. In short, there needs to be greater biological, epidemiological and health intelligence expertise in policing and national security intelligence agencies. The incorporation of additional specialists will provide policing and national security intelligence agencies with more focused threat

assessment, collection and analytical efforts for the prevention, detection and investigation of bioterrorism and biocrimes. In particular, based on much of the existing literature (which is lacking in any sophistication or precision about the nature of various biothreats), there is a critical need to more accurately estimate the risk and threat posed by biothreats. A more integrated role by epidemiologists, biologists and other public health experts in national security intelligence analysis and investigation will help to increase the accuracy or current calibration of biosecurity threats. Scientists can do this by helping to combine scientific disease modelling, biotechnology and biomedicine together with policing intelligence methodologies such as target profiling of offenders, and other evidence of conspiracy to use biological agents for malicious intent. Challenging, yet necessary questions need to be asked about the likelihood and capability of the use of various dangerous biological agents by various individuals or groups. For example, are the key biosecurity threats more likely to come from human transmission, zoonotic transmission, or via the environment, and what more can be done to assess their likelihood and capability using an amalgamated health and national security intelligence approach?

This second challenge is particularly important given in most cases a sudden disease outbreak frequently cannot be identified as deliberate or accidental, and disease experts will, at least in the first instance, be in a better position to track and interpret the significance of any biosecurity threat than their policing or national security intelligence colleagues. Additionally, enhanced levels of biosecurity expertise embedded with national security and policing intelligence agencies will be increasingly important in developing a more strategic approach to intelligence in the biosecurity context. Epidemiological modelling and some of the assessment work of future biological threats being sponsored by the DHS in the National Biodefense Analysis and Countermeasures programme, will also be useful in the early identification of other unintentional biological threats to humans, animals, plants and the environment. Some of these may not be terrorist-based, but many threats will still pose a worrying risk to national security and well-being. In summary, it is in this strategic space, where a threat has not yet actualized or caused harm that security and health intelligence principles can best be put to use to prevent, disrupt or contain myriad biosecurity threats, rather than merely reacting to a disease outbreak.

While it is desirable to increase the biosecurity intelligence capabilities of policing and national security intelligence agencies, the third challenge to overcome is to recognize and resolve differences between biological scientists and analysts working in traditional security contexts.

In Chapter 1, I described how the ‘culture of secrecy’ has defined strongly national security intelligence and policing practice. In contrast, the scientist tradition is marked by open enquiry, collecting and disseminating evidence in an open forum. So a key challenge will be to manage the different cultures, assumptions, priorities and even language between biological scientists and their national security and policing counterparts working on biosecurity issues. As noted earlier, some of these organizational cultural issues were on display during the 2001

anthrax investigation in the USA between CDC officers and FBI investigators. Not all these differences of course need to be resolved or are resolvable, but at the very least there needs to be a greater appreciation of what traditional intelligence and biological or biosecurity intelligence can bring to the table, and how each of these skill sets can inform better decision-making. Part of resolving some of the differences will obviously rely on a greater mutual understanding of skill sets.

For example, national security and policing analysts working in the biosecurity sector need to have at least a basic understanding of epidemiological principles, including their critical role in providing early warning of suspicious disease outbreaks, and their ability to model the trajectory of diseases. Biological scientists working on suspicious outbreaks need to understand various sensitive methodologies (for example, target profiling, covert sources and data matching), that their analytical cadre use to collect and analyse information on targets which may be intentionally releasing biological hazardous material into the environment. And there also needs to be a greater appreciation between the two that in some respects both health intelligence and national security intelligence analysts also use similar methodologies (e.g. geo-spatial information systems and analytics), albeit for different outcomes. A greater understanding between science and security colleagues of how similar and different methodologies are applied in various contexts, hopefully will result in a better integration of health and security techniques – allowing in turn for an improvement in the intelligence and evidence produced in biosecurity cases.

The fourth challenge that is obvious from the policy overviews for each country discussed above is information and intelligence sharing. To some extent, the information and intelligence sharing problem is not having necessarily insufficient intelligence, but in many cases there are too many sources of biosecurity information across a number of different systems. The diverse data sets dealing with biosecurity issues reflect in all these countries (some to a greater or lesser degree) the fragmented response to the issues among public and private agencies. Ideally, a more common biosecurity intelligence network that can move information and intelligence around between national security and policing agencies, scientists, public health officials and responders is required. There is a clear need to improve current biosecurity intelligence architecture and information management in order to maximize surveillance efforts against biosecurity threats in order to avoid a catastrophic biosecurity incident – intentional or otherwise. Nuzzo makes this point for the USA, arguing there is a need for one surveillance system rather than the many sometimes interoperable ones that currently exist. As Nuzzo suggests, 'It seems that one agency needs to take the lead in promoting better health information systems that can efficiently link health care and public health information' (2009: 37). Of course privacy issues arise here, and Americans have never been great fans of having their personal information, particularly health-related information, on government databases. But there does seem to be need for a system that can quickly move clinically relevant information from treating the individual patient to passing it on to other agencies if it has either broader public health significance, or is nationally significant from a biosecurity perspective. In the case of the USA, the

Department of Health should take on this health intelligence/information coordination role. But to be effective from a broader biosecurity perspective, relevant health care information needs to be better linked into the DHS intelligence network too, and this raises additional legal and governance challenges of possibly sharing some national security relevant information with scientists and clinicians in order to achieve better overall collection and analysis against a biosecurity threat.

In addition to developing national biosecurity intelligence and information networks that can allow real-time sharing of national security, policing and health intelligence, this system needs to promote better information sharing at the local levels. Again this is a challenge in any of the countries discussed above, given the large number of community, county, city, state and regional health departments, hospitals, public and private laboratories that may have useful information which could be swept up in any national biosecurity intelligence network. Again there are enormous challenges involved in just identifying what are the current platforms for data and information sharing and what are the legal, regulatory, liability issues relating to sharing of health data, criminal history information and top secret data (Tumin 2007: 10). One DHS-sponsored initiative to better integrate public health and community health interests into the broader Homeland Security information and intelligence sharing framework is the Health Security Intelligence Enterprise (HSIE), though this system is yet to become a fully developed framework to share health security information.

In the short to medium term though, perhaps in the case of the USA a more useful way to improve connectivity between those working on biosecurity in traditional intelligence agencies and those working on intelligence in the health or biology sector would be to maximize the latter's participation in the over 70 fusion centers established across the country – to better integrate counter-terrorism intelligence between federal, state and local authorities. Similar to the policing and national security agencies represented in fusion centers, health specialists can reach back into their own agencies and laboratories to source information which is directly relevant to assessing biosecurity threats.

Health authorities are in a position to more rapidly access and share information about suspicious disease outbreaks with their policing and national security intelligence partners, and this local information could more quickly be disseminated by DHS federally. Health experts could also contribute biosecurity expertise to any ongoing investigations generated from intelligence coming into the fusion center. Conversely the fusion center could prove to be an excellent structure to share relevant intelligence about various threat actors of concern to local health authorities, who will have a role in their containment or responding to them. In my visit to the Los Angeles fusion center (JRIC), it was pleasing to find that there is a registered nurse from the Los Angeles County Department of Public Health, and an analyst writing on a range of health security-related topics. In the case of Los Angeles too, the County Department of Public Health and the Los Angeles Field Office of the FBI have also established a technical advisory group to jointly share and analyse information that would allow the early detection and investigation of a WMD threat (Diamond and Kim 2010: 221). But it is not clear how other fusion

centers have included health specialists to work across biosecurity issues that are relevant to their national security and policing counterparts in these fusion centers. There is also the question of whether the health specialist staff seconded to a fusion center are the most appropriate people to provide the necessary expertise to their policing and national security counterparts. What kind of mix of health expertise might be appropriate, epidemiologists, registered nurses, physicians, biologists and why? We have seen from the discussion above that other countries have also tried other ways to 'fuse' biosecurity intelligence and information such as in the JTAC and the medical intelligence unit in the HPA, but it is not clear to what extent the work on collection, analysis and investigations supports across the spectrum of biosecurity issues other than bioterrorism.

## Conclusion

In conclusion, this chapter has focused on two emerging intelligence practice areas – one in the corrections and the other in the health context. Although the 'business' of corrections and biosecurity operate in very different environments, both reflect how intelligence capabilities are developing in non-traditional intelligence practice areas. In each sector there are significant challenges to the effective application of intelligence to inform decision-making. In corrections, there still remain in each of these countries concerns over the resourcing of intelligence functions to ensure adequate collection and analysis of threats at the operational, let alone at the strategic intelligence support level, for decision-makers. In many correctional environments, a fully developed intelligence framework is still not part, either by design or due to funding, of the core business. The growing concern in many prisons of increasing organized crime being conducted by offenders in prisons, and a greater need to understand levels of radicalization within prisons present complex challenges for the corrections environment. Such challenges will require the application of well-designed and well-run corrections intelligence programmes. Similarly, the biosecurity context, as discussed earlier, presents four key challenges for intelligence practice – some of these relate to definitional issues while others are more technical. At the definitional level, there is still an unresolved issue in many countries of what constitutes 'biosecurity'. This lack of certainty has clouded the policy response to biosecurity, and therefore which issues should be given priority and why. Not having a common policy understanding of what biosecurity is across the health and national security spectrums has also resulted in a fragmented intelligence response to the suite of potential threats. On a more specialized level, our discussion of policy developments above demonstrates that there are significant opportunities for national security agencies, policing and scientists to collaborate much more on biosecurity issues and investigations by using their specific approaches to intelligence. This is not to suggest, however, that such cooperation does not occur, merely that it needs to be more frequent and formalized in many cases.

To a large extent, the challenges identified in the corrections and biosecurity environments rest on the ability of political decision-makers and the executive

leadership of the agencies concerned to understand more clearly how intelligence can *enable* their decisions, and help predict new evolving threats in these emerging intelligence contexts. This in turn will rely on corrections and biosecurity agencies building holistic approaches to intelligence, and embedding them in their overall organizational structures, rather than seeing intelligence as just a tool to be used periodically.

An effective intelligence system can only work if it is part of the real-time decision-making environment, where intelligence assessments are integrated into other information feeds decision-makers are receiving. The current rhetoric in many countries about 'homeland security approaches', 'national resilience' or 'all hazards approaches' suggests that policy-makers have in mind the inclusion of some of these emerging practice intelligence areas into a broader response to contemporary security issues. The rhetoric is noble in practice. However, the traditional intelligence practice areas of national security and policing, with their own distinct 'intelligence traditions' (including long-held cultures of secrecy) will find it challenging to work with emerging practice areas which do not share this same 'tradition' and have new intelligence frameworks that are yet to fully reach their potential. But in the two examples discussed in this chapter, it is obvious there are increasingly more threat issues emerging in the security environment, which are of common concern for traditional intelligence players and emerging practice areas. It is therefore in the interest of maximizing our impact on various threats in the security environment, that academics and practitioners expand their normally narrow focus on just national security or policing intelligence to evaluate what is being done in emerging practice areas. There needs to be far more attention than there has been to date on how activity in emerging practice areas can be used in a more integrated way to improve overall the ability of all decision-makers to make a positive impact on the security environment. The other important reality is that emerging intelligence practice areas are shaking the boundaries of our previous understandings of what intelligence is all about in the post-9/11 environment and what we need to do to improve it.